代数学への誘い

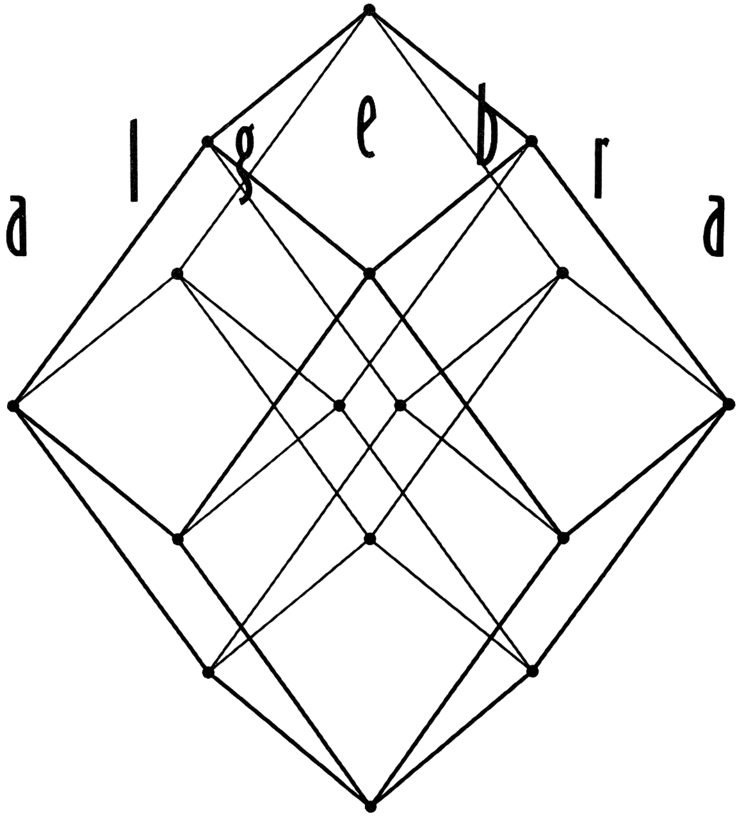


佐武一郎 著

遊星社

代数学への誘い

佐武一郎 著



遊星社

序

この本は，群とかガロア理論，イデアル論といった，いわゆる抽象代数学に興味をもっておられる方々になるべく広く，一体代数では何をどういうふうに考えるのかということを知っていただきたいと思って書いたものです．ですから特に予備知識は仮定せず，小学校のツルカメ算の話から始めました．最初の2章は，数学好きな一般の読者（A氏）やこれから数学の勉強を始めようとしている（高校や大学初年級の）学生諸君（Bさん，C君）を念頭において，抽象代数学がどういうものか，その考え方の違いや難点を説明したつもりです．第3章以下では，第2章の終わりのところで「おれは群論がわかったぞ！」と叫んだ人のために，さらに進んでいくつかのトピックスについて，代数的な考え方の説明を続けました．ここでえらんだ三つの話題「アーベル群の双対性」，「無限次ガロア理論」，「2次体・円分体の整数論」は一般の抽象代数の講義には含まれないことが多いのですが，抽象代数を整数論に適用しようとするとき，本質的に重要なものと思われます．したがって，やや専門的に代数を学ぼうとする読者にとって，通常の抽象代数学の講義を補足するものとして役立つことを期待しています．

こんなわけで，この本は抽象代数学の入門書でもなく，解説書でもなく，やや“あいまい”なものになってしまいました．しかし本当は，そこに著者のねらいがあるのです．抽象代数学の教科書は数多くありますが，その内容はやや類型的，辞書的で，限定されたものであり，形式的にも定義，定理，証明の連続でなかなか取り付き難いものです．（もちろん，数学科の学生諸君は

それを読まなければなりませんが.） 一方，解説書もたくさん出ていますが，こちらの方はいくぶん興味本意のものや歴史的説明が多く，数学的な考え方の面白さは実感として伝わってきにくいのではないでしょうか．この本ではそういう制約を離れて，もっと自由に読者と話をしたいと思いました．（少し悪いたとえで恐縮ですが）学生諸君をおいしい水場に連れてくることはなかなか大変ですし，水を飲ませることはいっそう難しい．結局，私たちにできることは貴方を自分の水場に案内して，何か話をしながら貴方が水を飲むのを待つことだけです．この本がそういう目的に少しでも役に立てば大変幸せです．

この本の性格上，系統的な説明や，定理の証明を省略して，特別な場合に制限したり，実例で説明したりしたところがいくつかあります．そういう点についてより詳しく知りたいと思う読者のために，「後書き」に最小限度の文献と引用をつけました．（本文中 * をつけた所です．） 参考にしていただければ幸いです．抽象代数学に関しては，（ここに挙げた［M］,［N］,［V］に限らず）何でも手近かにある本をとってみていただければ十分だろうと思います．

最後に遊星社の西原昌幸氏の数年にわたるご鞭撻とご協力に対し深く感謝いたします．

1995年10月

著　者

目　次

装丁＝海保　透
イラスト＝おやまだ祥子

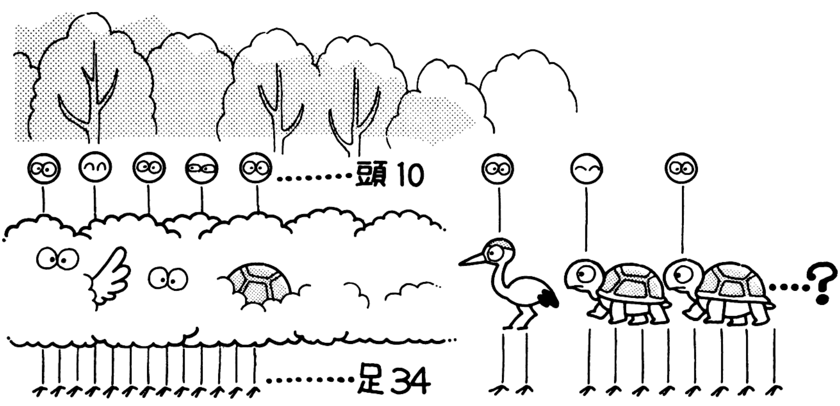
第1章　ツルカメ算から単因子論へ

1.1. 昔，私たちが小学生だったころ，ツルカメ算というものを習った．算数がまだ算術と呼ばれていた時代，東京の郊外の小川や池にまだ本物のカメが泳いでいた時代である．

ツルカメ算というのは，たとえば次のような問題を解く方法である．

「ここにツルとカメがいる．頭の数は全部で 10，足の数は全部で 34 である．ツルとカメはそれぞれ何匹か？」

これを解くには次のように考える．エート，ここにツルとカメがいるわけだが，もし全部がツルだったとすれば，足の数は $2\times10=20$ のはずである．ところが，実際には 34 である．この差 $34-20=14$ はカメが混じっているために起こる．ツルの代わりにカメが1匹入るごとに足の数は 2 だけ増える．それゆえカメは $14\div2=7$ 匹いなければならない．したがって，ツルは



$10-7=3$ 匹いることになる．よって，

答：ツル3匹，カメ7匹．

（ここで大切なことは，まずエートといって，“もし全部がツルであったならば”というように想像力を働かせるところである．）

1.2. さて中学に入ると，代数で方程式というものを習う．そこでは何でもわからないものを x とおき，問題の条件を式でかいてみる，すなわち，x のみたす方程式を作るのである．その方程式が解ければ，問題が解けたことになる．

このやり方でツルカメ算を考えてみよう．未知のもの，ツルの頭数を x，カメの頭数を y とする．そのとき

$$(\text{頭の総数}) = x+y,$$

$$(\text{足の総数}) = 2x+4y$$

であるから，与えられた条件を式でかけば，

$$x+y = 10, \tag{1}$$

$$2x+4y = 34 \tag{2}$$

という連立1次方程式がえられる．

この方程式を解く一番簡単な方法は未知数を一つずつ消してゆく方法，**消去法**である．（1）の両辺を2倍すると

$$2x+2y = 20 \tag{3}$$

となる．（2）から（3）を辺々引けば，x が消去されて

$$2y = 14,$$

したがって

$$y = 7.$$

（1）から

$$x = 10-y = 3$$

がえられる．

(この方法のよい点は，エートと考え込まなくても，自然に答がでてきてしまうところにある．しかし，よくよく見ると，なんと不思議なことに前と全く同じ計算をしているではないか．)

1.3. 高校に進むと，ベクトルと行列の演算，いわゆる線形代数を習う．

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \quad \begin{pmatrix} 5 \\ 6 \end{pmatrix}, \quad \begin{pmatrix} x \\ y \end{pmatrix}$$

のように，数または文字を正方形または長方形に並べたものを **行列**（マトリックス）という．$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ は2行2列の行列，または (2,2) 型の行列，$\begin{pmatrix} 5 \\ 6 \end{pmatrix}$ と $\begin{pmatrix} x \\ y \end{pmatrix}$ は2行1列の行列，または (2,1) 型の行列である．一般に，$(n, 1)$ 型の行列を n 次元の（列）ベクトルともいう．この本の読者は行列の演算についてはもうよくご存じだと思う．行列の和や積は

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}, \tag{4}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}, \tag{5}$$

$$\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x+x' \\ y+y' \end{pmatrix}, \tag{4'}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix} \tag{5'}$$

のように計算するのである．この計算に対しても通常の演算法則が成り立つ．たとえば，積 (5), (5′) に関する結合の法則

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right)\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\right) \tag{6}$$

が成り立つ．

また，特に行列 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ に対しては

$$(7) \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

$$(7') \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$$

が成り立つ．このように行列 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ は数の演算における 1 の働きをするので，**単位行列**と呼ばれている．(2,2) 型の単位行列を E_2 と書くことにする．

積の公式 (5) から，特に

$$(8) \qquad \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix}$$

がえられることに注意しておく．$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ を $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ の“随伴行列”という．

1.4. ツルカメ算に戻ろう．連立1次方程式 (1), (2)（ツルカメ方程式）の係数の行列

$$\begin{pmatrix} 1 & 1 \\ 2 & 4 \end{pmatrix}$$

を**ツルカメ行列**ということにする．ツルカメ方程式を行列の記号を使ってかけば，

$$(9) \qquad \begin{pmatrix} 1 & 1 \\ 2 & 4 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 10 \\ 34 \end{pmatrix}$$

となる．ここでツルカメ行列の随伴行列

$$\begin{pmatrix} 4 & -1 \\ -2 & 1 \end{pmatrix}$$

を（9）の両辺に（左から）掛ければ，左辺は（6）と（8）から

$$\left(\begin{pmatrix} 4 & -1 \\ -2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 2 & 4 \end{pmatrix}\right)\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2x \\ 2y \end{pmatrix}$$

となる．一方，右辺は

$$\begin{pmatrix} 4 & -1 \\ -2 & 1 \end{pmatrix}\begin{pmatrix} 10 \\ 34 \end{pmatrix} = \begin{pmatrix} 40-34 \\ -20+34 \end{pmatrix} = \begin{pmatrix} 6 \\ 14 \end{pmatrix}.$$

よって

$$\begin{pmatrix} 2x \\ 2y \end{pmatrix} = \begin{pmatrix} 6 \\ 14 \end{pmatrix}.$$

これから

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3 \\ 7 \end{pmatrix}$$

がえられる．よって，答：ツル 3 匹，カメ 7 匹．

（このように連立 1 次方程式は行列の計算によって，精確にいえば，次節で説明する逆行列を計算することによって，解くことができるのである．）

1.5. さて大学の数学科に入ると抽象代数学の講義をきくことになる．集合，写像，群などの概念が活躍する舞台である．話を進めるために，ここで簡単に群の概念を説明しておこう（詳しくは第 2 章を参照）．G を一つの集合，つまりあるものの集まりであるとする．さらに，G には一つの演算が定義されているとする．すなわち，G の元 a, b に対して，積 ab（または和 $a+b$）が定義されていて，次のような法則が成り立つものとする．

(i) 結合の法則 $(ab)c = a(bc)$ が成り立つ．

(ii) 単位元 1 が存在して，すべての元 a に対して $a1 = 1a = a$ が成り立つ．

(iii) 任意の元 a に対して，その逆元 a^{-1} が存在して，$aa^{-1} = a^{-1}a = 1$ が成り立つ．

このとき，G はこの演算に関して**群**になるというのである．（群の演算が和で与えられているときには，結合の法則は $(a+b)+c=a+(b+c)$ の形になる．また，単位元や逆元はそれぞれ 0（ゼロ），$-a$ とかく．）

たとえば，2次元ベクトル全体の集合を $\boldsymbol{R}^2$ とかくことにすれば，$\boldsymbol{R}^2$ の二つの元

$$\boldsymbol{x} = \begin{pmatrix} x \\ y \end{pmatrix}, \quad \boldsymbol{x}' = \begin{pmatrix} x' \\ y' \end{pmatrix}$$

に対して，その和が

$$\boldsymbol{x} + \boldsymbol{x}' = \begin{pmatrix} x+x' \\ y+y' \end{pmatrix}$$

によって定義される．この場合，(i) は明らかに成立する．(ii) は，単位元としてゼロベクトル $\boldsymbol{0} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ をとれば，

$$\boldsymbol{x} + \boldsymbol{0} = \boldsymbol{0} + \boldsymbol{x} = \boldsymbol{x}$$

であるから成立する．また $\boldsymbol{x} = \begin{pmatrix} x \\ y \end{pmatrix}$ に対して，$-\boldsymbol{x} = \begin{pmatrix} -x \\ -y \end{pmatrix}$ とおけば，

$$\boldsymbol{x} + (-\boldsymbol{x}) = (-\boldsymbol{x}) + \boldsymbol{x} = \boldsymbol{0}$$

であるから，(iii) も成立する．よって，$\boldsymbol{R}^2$ は加法に関して群になる．

同じようにして，(2, 2) 型の行列全体の集合も加法に関して群になる．それを $M_2(\boldsymbol{R})$ とかく．一般に加法に関する群を**加群**という．$\boldsymbol{R}^2$ も $M_2(\boldsymbol{R})$ も加群である．

さて $M_2(\boldsymbol{R})$ にはもう一つの演算，積，が定義されている．これに関しても (i) は成立している．また前に述べたように，E_2 を単位元として (ii) も成立する．すなわち，任意の (2, 2) 型行列 $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ に対して，

$$A \cdot E_2 = E_2 \cdot A = A \tag{10}$$

が成立する．（これは前に (7) とかいた式である．）しかし，任意の A に対

して逆元は必ずしも存在しない．実際，たとえば $A=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$ としたとき，もし $AX=E_2$ となるような行列 $X=\begin{pmatrix}x & y\\ z & t\end{pmatrix}$ があったとすれば，

$$AX=\begin{pmatrix}x & y\\ 0 & 0\end{pmatrix}=E_2=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

となってしまって矛盾である．（(2,2) 成分を比較すれば，$0=1$ がでる！）

前にあげた式 (8) からわかるように，$A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ に対して，もし $ad-bc\neq 0$ ならば，

(11)
$$A^{-1}=\begin{pmatrix}d(ad-bc)^{-1} & -b(ad-bc)^{-1}\\ -c(ad-bc)^{-1} & a(ad-bc)^{-1}\end{pmatrix}$$

とおくとき

(12)
$$A\cdot A^{-1}=A^{-1}\cdot A=E_2$$

が成立する．すなわち，$ad-bc\neq 0$ であるような行列 A は逆元 A^{-1} をもつ．$ad-bc$ を $A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ の **行列式** といい，$\det(A)$ で表す．明らかに $\det(E_2)=1$ である．（行列式の意味については「補遺 1」参照）

積の定義式 (5) から計算してみればわかるように，二つの (2,2) 型行列 A, B に対して

(13)
$$\det(AB)=\det(A)\cdot\det(B)$$

が成り立つ．よって，$\det(A)\neq 0$, $\det(B)\neq 0$ ならば，$\det(AB)\neq 0$ である．また，もし行列 A が逆元 B をもてば，$\det(A)\det(B)=1$．したがって $\det(A)\neq 0$, $\det(B)=\det(A)^{-1}$ である．以上により，行列式が 0 でないような (2,2) 型行列全体の集合は，乗法に関して群になることがわかる．この群を $GL_2(\boldsymbol{R})$ で表す．（第 2 章で説明する逆元の一意性により，A に逆元が存在すれば，それは (11) で与えられる A^{-1} と一致する．）

1.6. いままでの議論では，ベクトルや行列の成分はすべて実数と考えてきた．加群 $\boldsymbol{R}^2$ や $M_2(\boldsymbol{R})$ については，ベクトルや行列の成分をたとえば整数に制限してもやはり加群がえられる．これらの加群を $\boldsymbol{Z}^2$, $M_2(\boldsymbol{Z})$ で表す．($\boldsymbol{Z}$, $\boldsymbol{R}$ はそれぞれ整数全体の集合，実数全体の集合を表すブールバキの記号である.)

群 $GL_2(\boldsymbol{R})$ の元で成分が整数であるようなもの全体を考えると，それは乗法に関して閉じていて，条件 (i), (ii) は成立する．しかし，(iii) は一般に成立しない．たとえば，ツルカメ行列

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 4 \end{pmatrix}$$

に対して，$\det(A) = 2$ であるから

$$A^{-1} = \begin{pmatrix} 2 & -1/2 \\ -1 & 1/2 \end{pmatrix}$$

となり，この行列の成分は整数ではない．

もし A の成分も A^{-1} の成分も整数ならば，(12), (13) から

$$\det(A) \cdot \det(A^{-1}) = \det(E_2) = 1$$

となるから，$\det(A)$ は 1 の約数，すなわち ±1 でなければならない．逆に，行列 A の成分が整数で $\det(A) = \pm 1$ ならば，(11) からわかるように A^{-1} の成分も整数になる．そこで $GL_2(\boldsymbol{R})$ の元で，成分が整数で行列式が ±1 であるようなものをユニモジュラーといい，そのような (2,2) 型行列全体の集合を $GL_2(\boldsymbol{Z})$ とかくことにする．これに対しては条件 (i), (ii), (iii) が成立し，群になることがわかる．この群を（2次の）**モジュラー群**という．

1.7. さて群の説明が長くなってしまったが，再びツルカメ算に戻ろう．ツルカメ方程式（行列の形で (9)）を実数の範囲で解くためには，この式の両辺にツルカメ行列 $A = \begin{pmatrix} 1 & 1 \\ 2 & 4 \end{pmatrix}$ の逆行列 A^{-1} を掛ければよかった．しかし，A^{-1} の成分は整数ではないので，整数解を求めるためには一般により精密な

議論が必要になる．ツルカメ行列の場合，

$$\begin{pmatrix} 1 & 1 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \tag{14}$$

と分解され，第二の行列 $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ はユニモジュラーである．このことから，下に説明するように，ツルカメ方程式（9）の右辺のベクトルの第2成分，すなわちツルとカメの足の総数（上の例では 34）が偶数であるとき，またそのときに限って（9）は整数解をもつことがわかる．

一般の整数行列に対して，次の定理が成立する．

定理.* 成分が整数である $(2,2)$ 型の行列 A に対し，二つの（同じ型の）ユニモジュラー行列 U_1, U_2 があって

$$A = U_1\begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}U_2 \tag{15}$$

の形にかける．ここに d_1, d_2 は二つの負でない整数で，d_1 が d_2 の約数であるようにとることができる．そのとき，(d_1, d_2) は A によって一意的に定まる．

この (d_1, d_2) を行列 A の **単因子** * という．ツルカメ行列の単因子は $(1,2)$ である．

問題. 上の定理で単因子 (d_1, d_2) が一意的に定まる理由を考えてみて下さい．

（ヒント： d_1 は A の成分 a, b, c, d の最大公約数になる．それがわかれば，$d_1d_2 = |\det(A)|$ であるから d_2 の方も定まる．）

一般に成分が整数である $(2,2)$ 型行列 A に対して，ベクトル方程式

$$A\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} e \\ f \end{pmatrix} \tag{16}$$

が整数解をもつための条件を考えてみよう． A を（15）の形にかけば

$$U_1\begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}U_2\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} e \\ f \end{pmatrix}.$$

そこで

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = U_2 \begin{pmatrix} x \\ y \end{pmatrix}, \qquad \begin{pmatrix} e' \\ f' \end{pmatrix} = U_1^{-1} \begin{pmatrix} e \\ f \end{pmatrix}$$

とおけば，(16) は

$$(16') \qquad \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} e' \\ f' \end{pmatrix}$$

の形になる．U_2 がユニモジュラーだから，(16′) が x', y' に関して整数解をもてば，(16) も x, y に関して整数解をもち，その逆もいえる．(16′) は

$$\begin{cases} d_1 x' = e' \\ d_2 y' = f' \end{cases}$$

と同じことであるから，これが整数解をもつための必要十分な条件は e', f' がそれぞれ d_1, d_2 の倍数になることである．(したがって，整数解が存在するためには e, f がともに d_1 の倍数になることが必要である．)

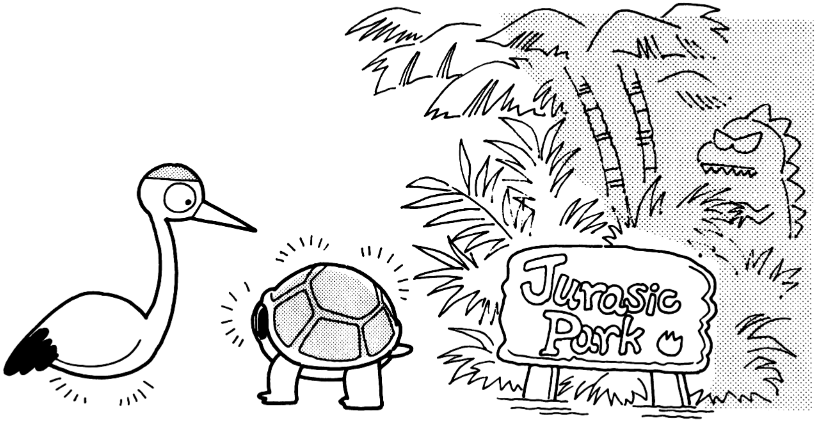
1.8. ここで話は変わるが，世はヴァイオテクノロジー（生物工学）の全盛時代である．遺伝子の組み替えによってトマトの巨木ができたりするときく．それならば，次のような空想的思考実験をしたとしてもまんざら非現実的とはいえないであろう．(実際，ジュラシック・パークの一隅ですでにこのような実験が密かに行なわれているかもしれない．)

ここに何匹かのツルとカメがいる．これから次のような法則に従って，新しい動物ツルリとカメラを作り出すことができると想像してみよう．

1. ツル x 匹とカメ y 匹から，ツルリ x' 匹とカメラ y' 匹ができるとすれば，(x', y') は (x, y) からモジュラー変換でえられる．すなわち，あるユニモジュラー行列 U があって

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = U \begin{pmatrix} x \\ y \end{pmatrix}$$

という関係が成立する．



ツルリとカメラ

2. ツルリには a 個の頭があるが足はなく，カメラには頭はないが，足が b 本ある．ここで a は b の約数である．

3. この生物学的変換に対して頭の総数と足の総数は不変である．

クイズ 1. この a, b を求めよ．（答は $(a, b) = (1, 2)$，すなわちツルカメ行列の単因子である．）

実際，条件 2, 3 により

$$ax' = x + y,$$
$$by' = 2x + 4y.$$

すなわち

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} U \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

これが任意の整数 $x, y \geqq 0$ に対して成立するから

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} U = \begin{pmatrix} 1 & 1 \\ 2 & 4 \end{pmatrix}$$

がえられる．(14) からわかるように，この方程式の解は

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \quad U = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

によって与えられる．この場合，これが（条件に適する）ただ一つの解であることもすぐにわかる．

クイズ2． ツル3匹，カメ7匹から何匹のツルリとカメラが生じるか？（答：ツルリ10匹，カメラ17匹.）

ツル，カメの代わりに他の動物を考えることもできる．しかし一般の場合には，条件3を次のように少し緩める必要がある：

3′．この生物学的変換に対して，頭の総数と足の総数とは一つのモジュラー変換を受ける．



ツルリとタコラ

例として，ツルとタコからツルリとタコラを作ることを考えてみよう．この場合，ツル・タコ行列は

$$\begin{pmatrix} 1 & 1 \\ 2 & 8 \end{pmatrix}$$

である．上と同様に考えれば，二つのユニモジュラー行列 U_1, U_2 があって，

$$\begin{pmatrix} 1 & 1 \\ 2 & 8 \end{pmatrix} = U_1 \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} U_2$$

が成立することになる．この方程式の一つの解は

$$U_1 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}, \quad U_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

で与えられる．すなわち，ツル・タコ行列の単因子は（1,6）である．これはタコラが（頭のない）6本足になることを意味する．この解を使えば，

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ y \end{pmatrix}$$

だから，ツル3匹，タコ7匹から，ツルリ10匹，タコラ7匹が生じる．

しかしたとえば，任意の整数 s に対して

$$\begin{pmatrix} 1 & 0 \\ -6s & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$$

が成立するから

$$U_1' = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -6s & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2-6s & 1 \end{pmatrix},$$

$$U_2' = \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ s & s+1 \end{pmatrix}$$

とおけば，これに対しても

$$\begin{pmatrix} 1 & 1 \\ 2 & 8 \end{pmatrix} = U_1'\begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}U_2'$$

が成立する．この解を使えば，

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ s & s+1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

だから，ツル3匹，タコ7匹のとき，ツルリは10匹であるが，タコラは（$7+10s$）匹も生じることになる！ このように U_1, U_2 のとり方はいく通りもあるから，与えられたツル，タコから生じるツルリ，タコラの数 x', y' を決めることはできない．しかし，上の定理によれば（a, b）=（1, 6）は一意的に決まる．これが単因子の生物学的意味（！）なのである．

第2章　抽象代数学の三つの難所

現在，大学の数学科で教える代数の主体はいわゆる「抽象代数学」である．これは数学であると同時に一つの語学というべきものであり，代数学はじめ数学全般を学ぶ上に必要な言語を身に付けさせることが，その目的の一つである．

抽象代数学ではまず，群，環，体，加群というような代数系の定義とその基本的な性質を学ぶ．これらはみな類似の言語系で，その始めの方は平行した構成になっている．これを並べてみると

群の定義 → 部分群，正規部分群 → 商群 → 群の準同型 → …

環の定義 → 部分環，イデアル → 商環 → 環の準同型 → …

というように進んでいく．

この章では群の場合を例にとり，この理論展開における“難所”を指摘してみたいと思う．明らかに難しい“難所”もあれば，一見それと気がつかない隠された“難所”もあるのである．

2.1. 群の定義.

まず群の定義から始めよう．

G を一つの集合とし，G の元を $a, b, \cdots, x, y, \cdots$ 等の文字で表す．G の二つの元 a, b の組に対し，その積と称する元 ab が定まるとき，すなわち，写像

$$G \times G \ni (a, b) \longmapsto ab \in G$$

が定義されているとき，G に一つの乗法が定義されているという．

定義 1. 集合 G に一つの乗法が定義されていて，次の条件が成立するとき，G は**群**であるという．

(G1)　任意の $a, b, c \in G$ に対し

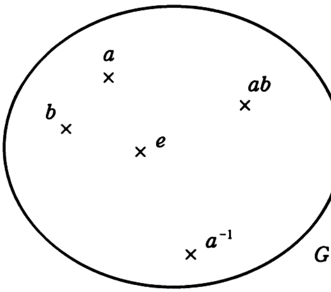
(1)
$$(ab)c = a(bc).$$

(G2) G の元 e が存在し，すべての $a \in G$ に対し

(2) $$ae = ea = a.$$

(G3) G の任意の元 a に対し，ある $a' \in G$ が存在し，

(3) $$aa' = a'a = e.$$



(G1) は結合律と呼ばれる．これは三つの元の積を作るとき，その順序さえ変えなければ，カッコをどのようにつけても，結果は同じであるという公理である．この条件を仮定しておけば，四つ以上の元の積についても同じことがいえる．たとえば，四つの元 a, b, c, d の（この順序の）積は5通りあるが，(1) を繰り返し適用すれば，それらがすべて相等しいことがわかる：

$$((ab)c)d = (a(bc))d = a((bc)d) = a(b(cd)) = (ab)(cd).$$

（このような一般の結合律は (G1) から帰納法によって証明される．）

(G2) の性質をもつ元 e を G の **単位元** という．単位元はただ一つしかない．実際，e, e' がともに単位元であるとすれば，

e が単位元であることから $ee' = e'$,

e' が単位元であることから $ee' = e$.

よって，$e = e'$ である．以下，G の単位元を e で表す．

(G3) における a' を a の **逆元** という．a の逆元はただ一つしかない．実際，a', a'' がともに a の逆元であるとすれば，

a' が a の逆元であることから $(a'a)a'' = ea'' = a''$,

a'' が a の逆元であることから $a'(aa'') = a'e = a'$.

(G1) により $(a'a)a'' = a'(aa'')$ であるから，$a' = a''$ がえられる．a の逆元を a^{-1} とかく．逆元について，次のような法則が成立する．

$$(ab)^{-1} = b^{-1}a^{-1}, \qquad (a^{-1})^{-1} = a, \qquad e^{-1} = e.$$

これらは (G1), (G2), (G3) を使って簡単に証明されるので，読者の演習問題ということにしておこう．

乗法の可換性 $ab = ba$ は一般に仮定しない．これが成立するとき，G を特に可換群またはアーベル群という．一般に加法は可換であると仮定しているので，加群は可換群である．

群の例としては，第1章，ツルカメ算の所で述べた $\boldsymbol{R}^2$, $\boldsymbol{Z}^2$, $GL_2(\boldsymbol{R})$, $GL_2(\boldsymbol{Z})$ 等をあげることができる．加群 $\boldsymbol{R}^2$, $\boldsymbol{Z}^2$ は可換群であるが，乗法群 $GL_2(\boldsymbol{R})$, $GL_2(\boldsymbol{Z})$ は非可換群である．

2.2. 部分群.　群 G の部分集合で，G と同じ乗法に関して群になるものを G の部分群という．正確にいえば，次のようになる．

定義2.　G を一つの群とする．G の（空でない）部分集合 H は次の条件をみたすとき，G の **部分群** であるという．

(S1)　$a, b \in H \Rightarrow ab \in H$.

(S2)　この乗法に関して (G1), (G2), (G3) が成立する．

(S2) において (G1) が成立することは仮定しなくてもよい．実際，すべての $a, b, c \in G$ に対して，(1) が成立するのであるから，すべての $a, b, c \in H$ に対しても (1) が成立するのは当然である．単位元，逆元の一意性によれば，H において (G2), (G3) が成立することは次のことを意味する．

(S2.1)　$e \in H$.

(S2.2)　$a \in H \Rightarrow a^{-1} \in H$.

実は $H \neq \phi$ と仮定すれば (S2.1) も不要である．実際，仮定によりある $a \in H$ が存在し，したがって (S2.2) により $a^{-1} \in H$．よって (S1) により

$$aa^{-1} = e \in H,$$

すなわち（S2.1）がえられる．

結論として，$H \subset G$, $H \neq \phi$ が部分群になるためには，(S1), (S2.2) が成立することが必要十分である．

たとえば，上の例の中で $\boldsymbol{Z}^2$, $GL_2(\boldsymbol{Z})$ はそれぞれ $\boldsymbol{R}^2$, $GL_2(\boldsymbol{R})$ の部分群である．

2.3. 商群. H を部分群とし，$a \in G$ に対し，

$$aH = \{ah \mid h \in G\}, \qquad Ha = \{ha \mid h \in G\}$$

で定義される集合を H の傍系（coset）という．普通，aH を右傍系，Ha を左傍系という．（この反対にいう人もいる．） すべての $a \in G$ に対して

$$aH = Ha \tag{4}$$

が成立するとき，H を G の **正規部分群** という．

上の例で $\boldsymbol{R}^2$ は可換群であるから，$\boldsymbol{Z}^2$ は $\boldsymbol{R}^2$ の正規部分群であるが，$GL_2(\boldsymbol{Z})$ は $GL_2(\boldsymbol{R})$ の正規部分群ではない．実際，$G = GL_2(\boldsymbol{R})$, $H = GL_2(\boldsymbol{Z})$,

$$a = \begin{pmatrix} 2 & 0 \\ 0 & 2^{-1} \end{pmatrix}, \quad a' = \begin{pmatrix} 0 & 2 \\ -2^{-1} & 0 \end{pmatrix} \ (\in G)$$

とおけば，

$$a^{-1}a' = \begin{pmatrix} 2^{-1} & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 0 & 2 \\ -2^{-1} & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in H,$$

$$a'a^{-1} = \begin{pmatrix} 0 & 2 \\ -2^{-1} & 0 \end{pmatrix}\begin{pmatrix} 2^{-1} & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 4 \\ -4^{-1} & 0 \end{pmatrix} \notin H$$

であるから，

$$a' \in aH, \quad \notin Ha.$$

よって，$aH \neq Ha$.

一般に，群 G の部分集合 A, B に対し

$$AB = \{xy \mid x \in A,\ y \in B\}$$

によってその積を定義する．特に $A = \{a\}$（一点からなる集合）のとき，

$AB = aB$ のようにかく.（上の傍系の記号はこの特別の場合である.）

さて H を G の正規部分群とし，二つの傍系

$$A = aH, \quad B = bH$$

の積を考える. $x \in A$, $y \in B$ は

$$x = ah, \quad y = bh', \quad h, h' \in H$$

とかけるから，

$$xy = ahbh'.$$

仮定（4）により，ある $h'' \in H$ があって $hb = bh''$. よって

$$xy = ab(h''h') \in abH.$$

したがって $aH \cdot bH \subset abH$ である. 逆に, $abH = a \cdot bH \subset aH \cdot bH$ は明らかであるから，

$$aH \cdot bH = abH \tag{5}$$

が成立する.

問題. 二つの相異なる傍系 A, B は共通元をもたない，いいかえれば（対偶），$A \cap B \neq \phi \Rightarrow A = B$ であることを示せ.

（ヒント： $x \in aH \Rightarrow xH = aH$ をいえばよい.）

さて，G の H に関する（右）傍系全体の集合を G/H とかく：

$$G/H = \{aH \mid a \in G\}.$$

（H が正規部分群であるから左傍系を考えても同じことである.） このとき，次の定理が成立する.

定理 1. H が G の正規部分群であるとき，傍系の集合 G/H は上に定義した積に関して群になる.

（証明） 条件（G1),（G2),（G3）を確かめればよい.

（G1） $A, B, C \in G/H$ を任意にとる.

$$A = aH, \quad B = bH, \quad C = cH$$

とすれば，

$$AB = abH, \quad (AB)C = (ab)cH,$$

$$BC = bcH, \quad A(BC) = a(bc)H.$$

G における条件（G1）により $(ab)c = a(bc)$ であるから，

$$(AB)C = A(BC)$$

がえられる．（実際，この関係は G の任意の部分集合 A, B, C に対して成立する．）

（G2） G/H の中には $H = eH$ が含まれている．すべての $A \in G/H$, $A = aH$ に対して

$$AH = aH \cdot eH = (ae)H = aH = A,$$
$$HA = eH \cdot aH = (ea)H = aH = A.$$

よって，H は G/H の単位元の条件をみたしている．

（G3） 任意の $A \in G/H$, $A = aH$ に対し，$A' = a^{-1}H$ とおけば，

$$AA' = aH \cdot a^{-1}H = (aa^{-1})H = eH = H,$$
$$A'A = a^{-1}H \cdot aH = (a^{-1}a)H = eH = H.$$

よって，A' は A の逆元になる． （証終）

（上記の A' を A^{-1} とかく．実際，$A^{-1} = \{x^{-1} \mid x \in A\}$ であることが示される．）

G/H を G の H による **商群** という．

2.4. 商群の例：$\boldsymbol{Z}/7\boldsymbol{Z}$.

$$G = \boldsymbol{Z} \quad （整数の加群），$$
$$H = 7\boldsymbol{Z} \quad （7 の倍数全体の作る部分加群）$$

とすれば，G は可換群であるから，H は正規部分群である．$G/H = \boldsymbol{Z}/7\boldsymbol{Z}$ の元は $a + 7\boldsymbol{Z}$ と表されるが，$a, a' \in \boldsymbol{Z}$ に対して，

$$a + 7\boldsymbol{Z} = a' + 7\boldsymbol{Z} \iff a - a' \in 7\boldsymbol{Z}$$

であり，$a - a' \in 7\boldsymbol{Z}$ は $a - a'$ が 7 の倍数であることを意味する．初等整数論では，この関係が成立するとき

(6) $$a \equiv a' \pmod 7$$

とかき，a と a' は7を法として合同であるという．したがってこの場合，$H=7\boldsymbol{Z}$ による傍系は“合同式”(6) によって定義される同値類（“剰余類”ともいう）に他ならない．

さて，任意の整数 a は

$$(7) \qquad a = 7q + r, \quad q, r \in \boldsymbol{Z}, \quad 0 \leqq r \leqq 6$$

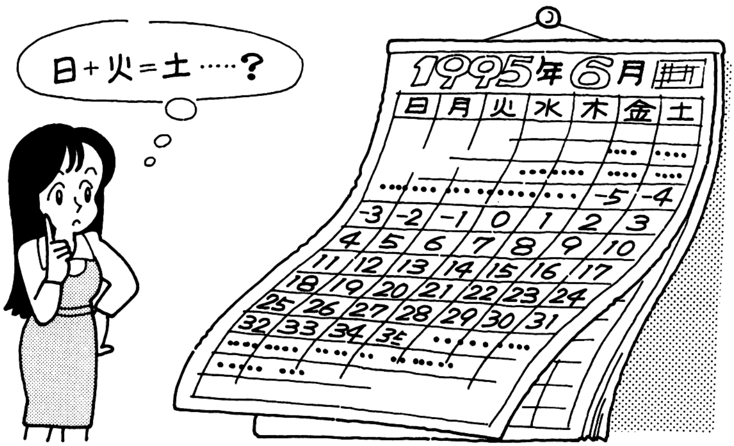
の形に一意的にかける（ユークリッドのアルゴリズム）．このとき

$$a + H = r + H$$

であるから，G の H による傍系（剰余類）のうち相異なるものは

$$r + H \qquad (0 \leqq r \leqq 6)$$

の7個であり，したがって商群 $G/H = \boldsymbol{Z}/7\boldsymbol{Z}$ は7個の元からなる有限群である．



これは今筆者の目の前にある今月（1995年6月）のカレンダーを前後に少し延長したものである．このようにしてできる無限カレンダーを想像すると，そのタテの列が mod 7 の剰余類，すなわち $H=7\boldsymbol{Z}$ による傍系であり，日月火水木金土はこれらの剰余類につけられた名称だということができる．

簡単のため，剰余類 $a+7\boldsymbol{Z}$ を $[a]$ とかくことにする．$\boldsymbol{Z}$ においてたとえば

$$4+6 \equiv 3 \pmod 7$$

であるから,

$$(4+7\boldsymbol{Z})+(6+7\boldsymbol{Z}) = 3+7\boldsymbol{Z},$$

すなわち, $\boldsymbol{Z}/7\boldsymbol{Z}$ において

$$[4]+[6] = [3]$$

が成り立つ.（1995年6月のカレンダーでは 日＋火＝土 である.） これらの式はみな同じことを表しているのである.

2.5. ラグランジュの定理. 群 G の元の個数が有限であるとき, G を有限群という. そのとき, G の元の個数を G の **位数**（または次数）といい, $|G|$ で表す.

G を有限群, H をその部分群とすれば, 明らかに H も有限群で, $|H| \leqq |G|$ である.

H が正規部分群であるとき, 商群 G/H は G の H による傍系の集合であるが, G が有限群ならば, 傍系も有限個しかないから, G/H も有限群である. その位数 $|G/H|$ は $|G|$ をこえない：$|G/H| \leqq |G|$.

さて, 三つの群 $G, H, G/H$ の位数の間には次の関係が成立する.

定理 2. G を有限群, H をその正規部分群とすれば, $|G| = |G/H| \cdot |H|$.

（証明） G の H による傍系のうち相異なるものを

$$a_1H,\ a_2H,\ \cdots,\ a_rH \qquad (r = |G/H|)$$

とする. また

$$H = \{h_1, h_2, \cdots, h_s\} \qquad (s = |H|)$$

とする. そのとき

$$a_iH = \{a_ih_1,\ a_ih_2,\ \cdots,\ a_ih_s\}$$

であるが, a_ih_j ($1 \leqq j \leqq s$) は相異なる.（もし $a_ih_j = a_ih_k$ ならば, 両辺に a_i^{-1} を左から掛けて $h_j = h_k$ を得る.） したがって, 各々の a_iH は（集合として）s 個の元からなる. G は部分集合 a_iH の共通部分のない和集合

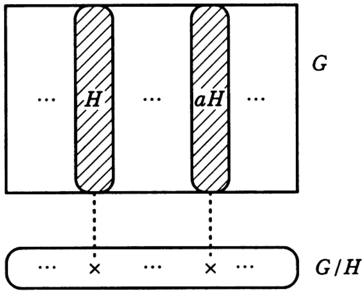
$$G = a_1H \cup a_2H \cup \cdots \cup a_rH$$

である（p.24の問題）から，その元の個数は全部で

$$|G| = rs = |G/H| \cdot |H|$$

である．　　　　（証終）

この定理を**ラグランジュ**（Lagrange）**の定理**という．$|G/H|$ を H の G における指数といい，通常 $[G:H]$ とかく．

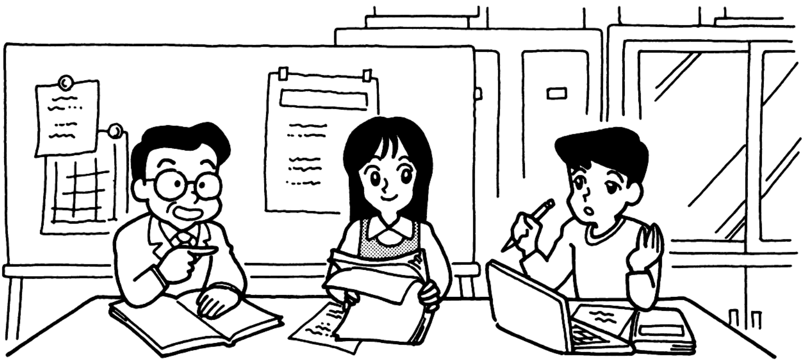


（商群 G/H の元は G の中の傍系 aH を一点とみなしたものである．）

2.6.　さてここまで，教科書ふうに群論の入り口のところを説明してきたが，ここでいったん休憩とし，本書の読者三人に登場してもらってその感想をきかせてもらうことにしよう．

＊　＊　＊

A氏「わしにはどうもよくわからない．なんでこんなに七面倒くさい議論をしなければならないのか？　これこれのものを群と定義するのはよろしい．実際，何をどう定義しようとわしは構わんからね．しかし，ある定理がいったん誰かによって証明されたとすれば，それはもう一つの真理なのではないかね？　それなら何もそうゴタゴタいわなくても，わしはそれを認めるのにヤブサカではない．君だってそれを認めているのだろう？　それならば，黙ってそれを覚えて何かに応用すればいいのではないのかね？　わしは忙しいのだ．」



Bさん「わたしにはいままでの議論はよくわかります．一つ一つ推論を追っていくとなるほどと思います．でもなんだか自分がベルト・コンベアに乗せられているようで，少し心もとない気もします．その motivation とかいうのかしら，なぜこういうものを考えなければならないかを説明していただけると有り難いんですけど．あの，わたし何かで読んだんですけど，群論はガロアというフランスの天才が発明したんですってネ．その人，21歳で決闘のために倒れてしまったんですってネ．まあ，なんてロマンチックなんでしょう．早くそのお話を聞かせてほしいわ．」

C君「僕も大体はわかるんですけれど，どうもところどころひっかかる所があるんです．一つの集合があって一つの演算が定義されているとか言われましたが，その集合は一体どこにあるんですか？ 実数とか行列とかの集合だったらまだわかるのですが，もっと一般のものを考えているのでしょう？ そんな一般なものを考えても大丈夫なんですか？ 現に商群 G/H は集合の集合なのでしょう．そうすると群の中にまた群が入っていて，そのまた中に群が入っているなんてことになって，フラクタルみたいで僕は頭がボーとしてしまうなあ．」

* * *

ごもっとも，ごもっとも．しかし私も神ならぬ身，諸兄姉の諸々のご不満

を一挙に解決することはとてもできません．どうかもう少しのご忍耐を．どうもみなさんが本書に期待しておられることと，私が説明しようと懸命になっていることの間には，少しずれがあるようだ．簡単に言ってしまえば，両方とも少々結果を急ぎ過ぎている．私の方は余計なことは言わないで，数学の話（定理や証明）だけを伝えたいと思っている．諸兄姉の方はあまり数学のことには頭を使わないで，その面白いところだけ聞きたいと願っている．ところが数学で一番肝心なところは，まさに私には説明ができないところ，諸兄姉がよけて通ろうとしているところ，つまり「数学がわかる」ということにあるのです．ちょうど，水泳を習おうとしている人に対して，私は黒板の前で図をかいて泳ぎ方を説明している，みなさんは水に濡れないで，珊瑚の海の景色を見たいと夢みているようなものです．一番大切な「泳ぐ」ということが抜けているのです．ちょっと目をつぶって水に入ってごらんなさい．案外簡単に泳げるようになるものです．よく赤ちゃんがプールで泳いでいる写真を見るでしょう．赤ちゃんはこわいもの知らずだから，かまわずボチャボチャし始めるのです．みなさんも赤ちゃんになったつもりで水に入ってしまうのがよいのです．

2.7. 定義について． 抽象代数に限らず数学を学ぶ上で，まず大切なことは，定義とはどういうものかを正しく認識することです．数学における「定義」とは一種の公理であって，それを基にして理論を展開させてゆくのです．「定理」は「定義」から論理的に（三段論法の積み重ねによって）「証明」されなければならないものです．したがって，数学を学ぶということは，「定理」を覚えることではなく，「証明」を理解すること，つまり自分で証明ができるようになることなのです．そして証明するためには，いつでも必要に応じて定義までさかのぼって考えることが大切です．自分で使ってみることによって初めて，定義の意味がわかってくるのです．

このことは数学者にとってはあまりにも自明なことなので，いまさら言う

までもないことのように思われるのですが，数学者以外の人には案外よく理解されていないようです．やはり数学は考えることを楽しむ学問なのですから，（A氏のような）お忙しい方もお暇なときにゆっくり考えていただきたいものです．最近では驚くべきことに，数学科の学生でさえ証明は苦手で，数学を暗記もののように思っている人がいます．学生もお忙しくなって考える暇がなくなってしまったのでしょうか．（昔は考えることが学生の存在意義だったと思うのですが．）それともこれも入学試験の影響なのでしょうか．

一方，定義はあくまでも数学の一つの素材にすぎないのですから，それについて文学的，哲学的に考えても無意味です．（C君のように）あまり深刻に考えずに，定義は素直に受け入れる方がよい．もちろん，十分に限定された範囲で考えなくてはいけない．たとえば，「すべての群の集合」などというものを考えれば，たちまち集合論的矛盾にぶつかってしまうでしょう．

定義（公理）は簡単明瞭で，しかもその内容が豊富であることが望ましい．ユークリッド幾何の公理はその一つの典型です．群の公理も実に簡単ですが，そこから導き出される結果は膨大なものです．有限単純群の分類論は今世紀数学の一つの大きな収穫ですが，その証明を全部書き上げれば（それができたとしての話ですが）何千ページにもなるだろうと言われています．

定義のもつ意味を正しく認識すること．これが抽象代数学の出発点であり，最初の難所なのです．この難関を通り抜けないと抽象代数の中に入っていくことはできないのです．これは人があまり気づいていない，しかしおそらく一番重要な難所だろうと思います．

2.8. 余談. 少し余談になりますが，私も最近は必要にせまられて，少しばかりパソコンをいじくるようになりました．そうはいっても，私の場合，単にワープロとして手紙や論文を打つだけのことです．私は大学にいますから，機器の類はたいてい助手のような人が据え付けてくれます．急に機械が動かなくなって困ったような時には，必ず隣の部屋に親切な同僚がいて，助けに

来てくれます．私はただ彼の指が魔法のごとく動くのを感心して眺めているばかりです．

しかしそれでも時にはどうしても例の「マニュアル」と称する本を読まなければならなくなります．この悪名高い「マニュアル」はほとんど読者に対して敵意をもって書かれたのではないかと思われるほどわかりにくい．たいていの場合は数頁（または数行）読むだけで絶望してしまい，翌朝また親切な同僚を探しにいって教えを乞うということになります．

そこで卒然と気がついたのですが，学生諸君が数学がわからないというのも，これと同じことなのではないでしょうか．違うのはただ私が親切な同僚を探すかわりに，学生たちは宿題の問題を説明してくれる親切な先生を見つけるというところだけです．（私もC大学では親切な先生の一人なのです．）

パソコンのことがわかる人は，実はマニュアルなど読まなくても始めからわかっている．それと同じように数学がわかる人には勉強する前から数学がわかっている（あるいはわかるようにできている）のです．逆に，私がパソコンがわからなくて足掻(あが)いているように，多くの学生諸君は数学を理解する糸口がつかめなくて困っているのです．



しかし数学の教科書は（少なくとも私たちの大学で使うような教科書は），パソコンのマニュアルとは違って，読めばわかるように書いてあるはずです．

いうならば self-contained に，実に懇切丁寧に書いてあります．それがわからないのは，どういうわけでしょうか．

そこでまた思い当たるのですが，パソコンで書き込むときには必ずフロッピーディスクを使います．これがまた面倒なことにそれぞれ独自のフォーマットがあって，フォーマットが違うとどうしても読み出すことも書き込むこともできません．数学がわからないという人は，きっと頭が数学を受け入れるようにフォーマットされていないのだと思います．（これは頭がいいとか悪いとかいうのとは全く無関係です．）数学を受け入れるためには前節で述べたように，邪念を捨て，気を落ち着けて，素直に，しかし論理的に，デカルト的に，書いてあることについて考える態度が必要なのです．そのようにして読めば，（Bさんのように）抽象代数などは意外にやさしいことに気がつくでしょう．

考えてみると，私たちは結局，自分の頭のフォーマットに適合した本しか読まないようにできているのだと思います．ある小説が面白いのはそれがその人のフォーマットによく合っているからです．友人が面白いから読めという本が私にも面白いことはめったにありません．逆に，たとえば私にとっては難解そのものであるような小説を書く，大江健三郎氏がノーベル賞を受賞したとしても別になんの不思議もないわけです．逆説的にいえば，万人に読まれるベストセラーというものは一番面白くない本ということになるでしょう．

2.9. 商群の落とし穴. さて第一の関門を無事通り抜けて，群の基本概念，部分群，と理解を深めてこられた読者も商群のところでちょっと戸惑ったのではないでしょうか？ 商群 G/H の“元”は aH で，それは一つの傍系ですから，それ自身一つの集合です．つまり，商群 G/H はC君がいうように集合の集合なのです．

ここで一つの思考の飛躍が必要となる．個々の傍系 aH は集合であるが，集

合 G/H を考えるときには，aH はその元であり，点のようなものです．ちょうど，地球とか，火星とかはそれぞれたくさんの元素の集合体ですが，太陽系という視点でみるならば，地球や火星は点だと考えるのに似ています．さらに銀河系を考えるときには，太陽系も（他の多くの太陽系と同じように）それを構成する点のようなものと考える．このように視点を変えることによって，同じものを集合と考えたり，元（点）と考えたりすることは，日常生活でも無意識のうちによく行なわれていることです．

しかしよく考えてみると，そこに少し違いがあることに気がつくでしょう．たとえば，日常生活で“人間の集合”というとき，それはあくまでも大きさのある，生きた（または死んだ）人間の集まりを考えているのですが，（もしそうでなければ，お前は非人間的な奴だとおこられてしまうでしょう），数学で“人間の集合”というときには，個々の人間はもはや大きさのない一つの元，または点としか考えないのです．（数学をするときには，人間ではなく神になったような気持ちでなければいけない！）ここに一つの思考の飛躍があることをはっきり認識しないと，とんでもない混乱に陥ってしまいます．

ラグランジュの定理（2.5節）の証明の中で，商群 G/H の元 a_iH は s 個の元からなる集合ですが，それを商群 G/H の元とみるとき，それは一個の元であり，したがって G/H は r 個の元からなる集合である．それに対してもとの群 G は s 個の元からなる傍系 r 個の和集合ですから全体として rs 個の元からなっているのです．

別の例で説明しましょう．2次元のベクトル

$$\boldsymbol{a} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$$

は二つの実数 a_1, a_2 の（順序のついた）集合として定義されています．しかしそれは平面 $\boldsymbol{R}^2$ の点を表している．つまりベクトル $\boldsymbol{a}$ を一つだけ考えるとき，それは0次元のものなのです．このようなベクトルを全部考えるならば，

すなわち集合

$$\{\, \boldsymbol{a} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \mid a_1, a_2 \in \boldsymbol{R} \,\}$$

を考えれば，初めてそれは2次元の平面 $\boldsymbol{R}^2$ になるわけです．

Bさんのように，ベルト・コンベアに乗った気持ちであまりにスラスラと受け入れてしまうと，この“点 $\boldsymbol{a}$”と“平面 $\boldsymbol{R}^2$”の区別がつかなくなり，あとから「エエ，集合の集合ですって？」と目を白黒させることになってしまいます．

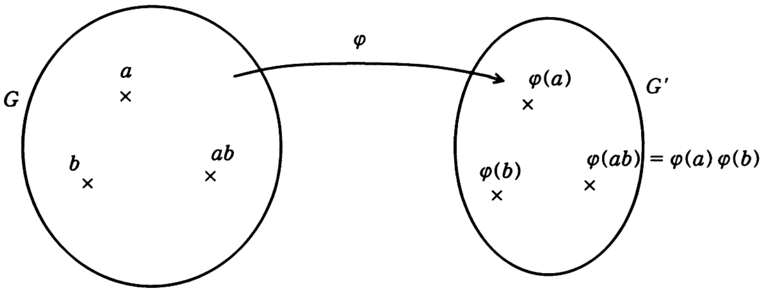
商群という概念にひそむこの落とし穴を“飛躍”することが，抽象代数学の第二の難所なのです．

2.10. 群の準同型. 抽象代数ではその対象である群や環の間の写像を考えることが重要である．群論においては，群の構造を保つ写像を群の準同型という．正確にいえば，次のようになる．

定義3. G, G' を二つの群とする．G から G'（の中）への写像 φ は，任意の $a, b \in G$ に対して，条件

(8) $$\varphi(ab) = \varphi(a)\varphi(b)$$

をみたすとき，G から G' への **準同型** であるという．



(8) の左辺の積 ab は群 G における積であり，右辺の積 $\varphi(a)\varphi(b)$ は群 G' における積である．したがって，(8) は写像 φ が群の演算を保つことを表し

ている．

G, G' の単位元を e, e' とすれば，

(9)
$$\varphi(e) = e'$$

が成立する．実際，$ee = e$ であるから，(8) により

$$\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e).$$

したがって，両辺に $\varphi(e)^{-1}$ を掛ければ，

$$e' = \varphi(e)^{-1}\varphi(e) = \varphi(e)^{-1}\varphi(e)\varphi(e) = e'\varphi(e) = \varphi(e)$$

となり，(9) がえられる．

また，任意の $a \in G$ に対して

(10)
$$\varphi(a^{-1}) = \varphi(a)^{-1}$$

が成立する．実際，$a \cdot a^{-1} = e$ の両辺に φ を施せば，(8), (9) により

$$\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(e) = e'.$$

よって，$\varphi(a)^{-1} = \varphi(a^{-1})$ がえられる．

準同型 φ が G から G' の上への一対一写像であるとき，**同型**であるという．同型 $\varphi: G \to G'$ が存在するとき，“二つの群 G, G' は同型である”といい，$G \cong G'$ とかく．(φ が同型であるとき，逆写像 φ^{-1} も同型になる．このことから，群の同型は一つの同値関係になることが証明される．)

2.11. 準同型定理.　準同型 $\varphi: G \to G'$ が与えられているとき，

$$\mathrm{Ker}\,\varphi = \{ x \in G \mid \varphi(x) = e' \},$$

$$\mathrm{Im}\,\varphi = \{ \varphi(x) \mid x \in G \}$$

とおく．Ker は Kernel (核) の略，Im は Image (像) の略である．このとき次の定理が成立する．

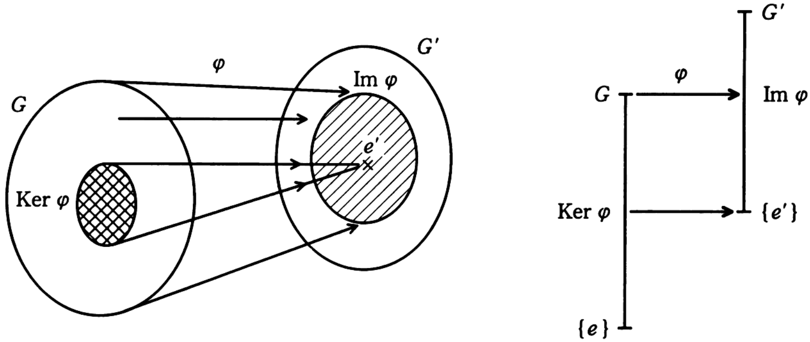
定理 3.　$\mathrm{Ker}\,\varphi$ は G の正規部分群，$\mathrm{Im}\,\varphi$ は G' の (ただの) 部分群で，対応

(11)
$$a \cdot \mathrm{Ker}\,\varphi \longmapsto \varphi(a) \qquad (a \in G)$$

により，同型

(12) $$G/\mathrm{Ker}\,\varphi \cong \mathrm{Im}\,\varphi$$

が成立する.



（証明） $N = \mathrm{Ker}\,\varphi$ とおく．まず，N が G の部分群であることをいう．そのためには，条件（S1),（S2.1),（S2.2）が成立することをみればよい．

（S1）の証： $a, b \in N \Rightarrow \varphi(ab) = \varphi(a)\varphi(b) = e'e' = e' \Rightarrow ab \in N$.

（S2.1）の証： 上記の（9）により $e \in N$.

（S2.2）の証： （10）により

$$a \in N \implies \varphi(a^{-1}) = \varphi(a)^{-1} = e'^{-1} = e' \implies a^{-1} \in N.$$

次に $a \in G,\ x \in N$ とすれば，

$$\varphi(axa^{-1}) = \varphi(a)\varphi(x)\varphi(a)^{-1} = \varphi(a)\varphi(a)^{-1} = e'.$$

よって $axa^{-1} \in N$ すなわち $aNa^{-1} \subset N,\ aN \subset Na$．同様にして，$a^{-1}xa \in N$ から $Na \subset aN$ がえられる．よって，$aN = Na$，すなわち N は正規部分群である．

$\mathrm{Im}\,\varphi$ が G' の部分群になることの証明は省略する．（読者の演習としよう.）

さて，$a,\ a' \in G$ に対して

$$\varphi(a) = \varphi(a') \iff \varphi(a^{-1}a') = e' \iff a^{-1}a' \in N \iff aN = a'N$$

であるから，対応 $aN \leftrightarrow \varphi(a)$ は代表 a のとり方に関係なく定まり（いわゆる well-defined で)，G/N と $\varphi(G) = \mathrm{Im}\,\varphi$ の一対一の対応を与える．明らかに，

$$aN \longleftrightarrow \varphi(a), \quad bN \longleftrightarrow \varphi(b)$$

のとき

$$aN \cdot bN = (ab)N \longleftrightarrow \varphi(ab) = \varphi(a)\varphi(b)$$

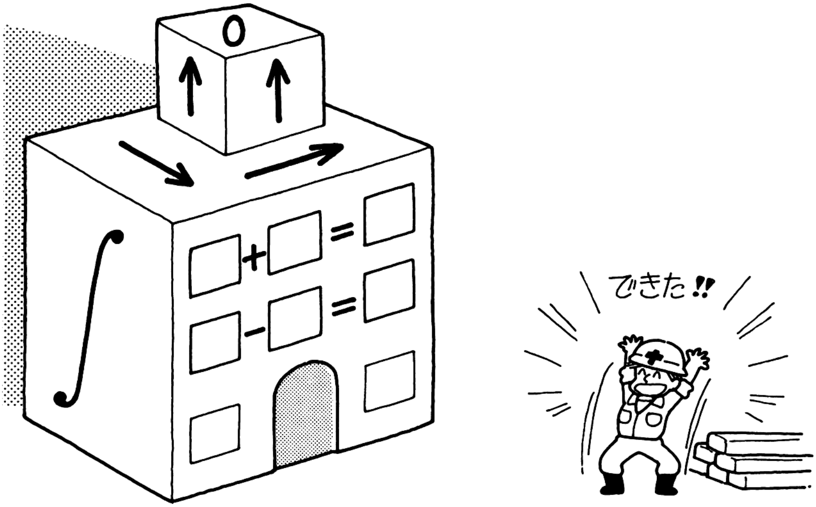
であるから，この対応は（どちらの向きにも）準同型である．よって

$$G/N \cong \operatorname{Im} \varphi. \qquad \text{（証終）}$$

2.12. 抽象代数学のロマン． いま説明した準同型の概念，それと商群とを結びつける準同型定理，これらがよく理解され活用されるようになれば，万々歳，「おれは群論がわかったぞ！」と叫ぶことができる．逆に，群論がわかるためには，どうしてもこの準同型の概念，準同型定理を理解しなければならない．これが第三の難関なのです．

始めに言ったように，群論も環論も加群の理論も最初のところは平行しているから，群論の準同型定理がわかれば，環論の準同型定理も加群の準同型定理もみな同じように理解できるわけです．商や準同型の定義は少しずつ違うのですが，考え方の基本は全く同じなのです．

これも前に言いましたが，集合とか写像とかいうものは日常生活でもよく使う概念です．ある大学の学生の集合，その中の x 学科 y 年生の学生が作る部分集合，その学生について何か（たとえば身長）を測れば，それは学生に実数を対応させる写像（関数）を定義したことになる．数学で扱う集合や写像もこれと同じことで，概念的には別に新しいものではない．しかし，日常生活ではこれをやや曖昧に（人間的な意味に）使うのに対して，数学ではこれらの概念を非常に限定された，明確な（神的な）意味に使うのです．それは一見不自由そうに見えますが，実際には，逆にこの厳密さのゆえに，これらの概念を組み合わせて，非常に精巧な大理論を構築することが可能になる．そこに数学者の大きなロマンがあるのです．ちょうど作曲家の発想が精密な楽譜によって記述されるように，数学者の夢は抽象代数学を使って組み立てられた堅固な建築物として実現されるのです．



2.13. 再びツルカメ算. 群論の基礎概念を学んだ上で，もう一度ツルカメ算を思い出してみよう．

ツルカメ算は結局

$$A\boldsymbol{x} = \boldsymbol{b}, \quad A = \begin{pmatrix} 1 & 1 \\ 2 & 4 \end{pmatrix}, \quad \boldsymbol{b} = \begin{pmatrix} 10 \\ 34 \end{pmatrix}$$

のようなベクトル方程式を解くことであった．ツルカメ行列 A は写像

(13) $$\psi_A : \boldsymbol{x} \longmapsto A\boldsymbol{x}$$

を定義する．ここで $\boldsymbol{x}$ が $\boldsymbol{R}^2$ を動くものと考えれば，これは加群（またはベクトル空間）$\boldsymbol{R}^2$ からそれ自身への準同型（すなわち自己準同型）であるが，$\det(A) = 2 \neq 0$ であるから，逆行列 A^{-1} が存在し，

(14) $$\psi_{A^{-1}} : \boldsymbol{x} \longmapsto A^{-1}\boldsymbol{x}$$

は ψ_A の逆写像になっている．（すなわち，$\psi_A \circ \psi_{A^{-1}} = \psi_{A^{-1}} \circ \psi_A = 1$ が成立する．）したがって，ψ_A は $\boldsymbol{R}^2$ の自分自身の上への同型（すなわち自己同型）になる．

しかし $\boldsymbol{x}$ が $\boldsymbol{Z}^2$ を動くと考えれば，すなわち ψ_A の $\boldsymbol{Z}^2$ への制限を考えれば，

$$\psi_A(\boldsymbol{Z}^2) = A\boldsymbol{Z}^2 \subsetneq \boldsymbol{Z}^2$$

であるから，ψ_A は $\boldsymbol{Z}^2$ の自己準同型ではあるが，自己同型にならない．このことをより詳しくみるために，ツルカメ行列の単因子分解

$$A = DU = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

を使って，ψ_A を二つの準同型

$$\psi_D : \boldsymbol{x} \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\boldsymbol{x}, \qquad \psi_U : \boldsymbol{x} \longmapsto \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}\boldsymbol{x}$$

の積に分解する：$\psi_A = \psi_D \circ \psi_U$．そのとき $U = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ はユニモジュラーであるから，対応する準同型 ψ_U は $\boldsymbol{Z}^2$ の自己同型になる．一方，ψ_D については

$$\mathrm{Im}\ \psi_D = \{ \begin{pmatrix} x_1 \\ 2x_2 \end{pmatrix} \mid x_i \in \boldsymbol{Z} \},$$

$$\mathrm{Ker}\ \psi_D = \{\boldsymbol{0}\}$$

である．したがって

$$A\boldsymbol{Z}^2 = D(U\boldsymbol{Z}^2) = D\boldsymbol{Z}^2 = \boldsymbol{Z} \times 2\boldsymbol{Z}$$

である．

一般に $A \in M_2(\boldsymbol{Z})$ を

(15)　　$A = U_1 D U_2, \quad U_1, U_2 \in GL_2(\boldsymbol{Z}), \quad D = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix}$

と分解すれば，対応する準同型は

$$\psi_A = \psi_{U_1} \circ \psi_D \circ \psi_{U_2}$$

と分解される．ψ_{U_1}, ψ_{U_2} は $\boldsymbol{Z}^2$ の自己同型であるが，ψ_D については

$$\mathrm{Im}\ \psi_D = \{ \begin{pmatrix} a_1 x_1 \\ a_2 x_2 \end{pmatrix} \mid x_i \in \boldsymbol{Z} \} = a_1\boldsymbol{Z} \times a_2\boldsymbol{Z}.$$

したがって，

$$AZ^2 = U_1DU_2Z^2 = U_1DZ^2.$$

Z^2 の自己同型 $\psi_{U_1}^{-1}$ により，U_1DZ^2 は DZ^2 にうつされるから，この対応により $AZ^2 \cong DZ^2$ となる．よって商群 Z^2/AZ^2（ψ_A の cokernel）を考えれば，

(16) $$Z^2/AZ^2 \cong Z^2/DZ^2 \cong (Z/a_1Z) \times (Z/a_2Z)$$

である．

よって，“行列 A の単因子が（a_1, a_2）である”ということは“加群 Z^2/AZ^2 が二つの巡回群 Z/a_1Z と Z/a_2Z の直積になる”ということを表している．また，$a_1a_2 > 0$ ならば，

$$|Z^2/AZ^2| = a_1a_2 = \det(A)$$

である．（補遺 1 参照）

一般に次の定理が成立する．

定理 4． 有限アーベル群 G はいくつかの巡回群

$$G_i \cong Z/a_iZ \quad (1 \leqq i \leqq s), \qquad a_i > 1,$$

の直積として表される．このとき a_i（$1 \leqq i \leqq s-1$）を a_i が a_{i+1} の約数になるようにとることができる．またこの条件の下に $\{a_i\ (1 \leqq i \leqq s)\}$ は一意的に定まる．（($a_1, \cdots, a_s$) を G の“型”という．）

これが **(有限) アーベル群の基本定理*** である．（$a_i = 0$, $G_i \cong Z$ の場合も含めることにすれば，同じ形の定理がより一般に有限生成のアーベル群に対しても成立する．）上に説明したように，整数行列の単因子論はこのアーベル群の基本定理を行列の言葉でいい代えたものに他ならない．

第3章　代数における双対性

代数学において考える対象（群，環，体，ベクトル空間など）の中には，二つのものが一つの対になって現れる場合がしばしばある．そのときそれらを同時に考えるとその構造がいっそう明瞭になる．このような現象は一般に“双対性”と呼ばれている．その典型的な例は有限アーベル群の双対性であろう．（別の例はガロア理論である！）それについて一番簡単な巡回群の場合に説明することにしよう．

3.1．巡回群．　G を一つの群とする．$a \in G$ をとり，a のベキ

$$a, a^2, a^3, \cdots$$

を考える．一般に，正の整数 m に対し，ベキ a^m を $a^m = a^{m-1} \cdot a$ によって帰納的に定義するのである．さらに

$$a^0 = e \text{（単位元）},$$
$$a^{-1} \text{（} a \text{ の逆元）},$$
$$a^{-2} = (a^{-1})^2 = (a^2)^{-1}, \quad \cdots\cdots,$$

一般に $a^{-m} = (a^{-1})^m \; (= (a^m)^{-1})$ として，負のベキも定義される．［等式 $(a^{-1})^m = (a^m)^{-1}$ は群の公理から帰納法によって簡単に証明される．］このように定義された一般のベキについて“指数法則”

(1)　$$a^m \cdot a^n = a^{m+n}, \qquad (a^m)^n = a^{mn} \qquad (m, n \in \boldsymbol{Z})$$

が成り立つことが証明される．（しかしここではこれらの証明には立ち入らないことにする．）これらのことからただちに次の定理がえられる．

定理1．　G を群，$a \in G$ とすれば，a のベキ全体の集合

$$\{ a^m \mid m \in \boldsymbol{Z} \}$$

は G の部分群になる．（この部分群を $\langle a \rangle$ とかくことにする．）

特に $G = \langle a \rangle$ となるとき，G を a によって生成される**巡回群**という．

一般に，$\langle a \rangle$ において

$$a^m = e$$

となるような正の整数 m が存在する場合と存在しない場合とがある．前の場合，そのような m の中で最小のもの n を a の位数（order）という．後の場合，a の位数は ∞ であると定義する．記号でそれぞれ $\mathrm{ord}\, a = n, \infty$ とかく．

定理 2. a の位数を $n < \infty$ とすれば，

$$\langle a \rangle = \{e, a, \cdots, a^{n-1}\}$$

であり，a^i（$0 \leqq i \leqq n-1$）は相異なる．（したがって，$|\langle a \rangle| = n$ である．）

（証明） これは簡単な定理であるが，第2章，準同型定理を使って証明してみよう．$\boldsymbol{Z}$ を整数全体の作る加群とし，写像

$$\varphi : \boldsymbol{Z} \ni m \longmapsto a^m \in G$$

を考える．(1) により φ は（加群 $\boldsymbol{Z}$ から乗法群 G への）準同型で，その像 $\mathrm{Im}\, \varphi$ は $\langle a \rangle$ である．ユークリッドのアルゴリズムにより，$m \in \boldsymbol{Z}$ を

$$m = qn + r, \qquad 0 \leqq r \leqq n-1$$

とかけば，$a^n = e$ であるから，

$$a^m = (a^n)^q a^r = a^r.$$

よって

$$a^m = e \iff a^r = e \iff r = 0 \iff m = qn.$$

いいかえれば，$\mathrm{Ker}\, \varphi = n\boldsymbol{Z}$．したがって準同型定理により

$$\langle a \rangle \cong \boldsymbol{Z}/n\boldsymbol{Z} = \{[0], [1], \cdots, [n-1]\}.$$

この同型対応は $a^i \leftrightarrow [i]$（$= i + n\boldsymbol{Z}$）によって与えられる．よって

$$\langle a \rangle = \{e, a, \cdots, a^{n-1}\},$$

特に $|\langle a \rangle| = n$ である． （証終）

同様に，a の位数が ∞ のときには，$\langle a \rangle \cong \boldsymbol{Z}$ である．まとめていえば，

(2)
$$\langle a\rangle \cong \begin{cases} \boldsymbol{Z}/n\boldsymbol{Z} & \text{ord}\, a = n \text{ のとき,} \\ \boldsymbol{Z} & \text{ord}\, a = \infty \text{ のとき.} \end{cases}$$

3.2. 指標群.　絶対値 1 の複素数全体のつくる乗法群を $\boldsymbol{C}^{(1)}$ とかくことにする.

G を一つの群とする. $\boldsymbol{C}^{(1)}$ に値をもつ G 上の関数 χ で

(3)
$$\chi(xy) = \chi(x)\cdot\chi(y) \qquad (x, y \in G)$$

をみたすもの, すなわち準同型写像

$$\chi : G \longrightarrow \boldsymbol{C}^{(1)}$$

を G の **指標** という.

定理 3. 群 G の指標全体は, 関数としての乗法に関して群になる. (それを $\widehat{G}$ とかく.)

実際, χ, χ' を G の指標とするとき

(4)
$$(\chi\chi')(x) = \chi(x)\cdot\chi'(x) \qquad (x \in G)$$

によって積を定義すれば, $\chi\chi'$ も $\boldsymbol{C}^{(1)}$ に値をもつ G 上の関数で

$$\begin{aligned}(\chi\chi')(xy) &= \chi(xy)\cdot\chi'(xy) \\ &= \chi(x)\chi(y)\chi'(x)\chi'(y) \\ &= \chi(x)\chi'(x)\chi(y)\chi'(y) \\ &= (\chi\chi')(x)\cdot(\chi\chi')(y).\end{aligned}$$

よって, $\chi\chi'$ も G の指標である. この積に関して群の条件が成立することは容易に確かめられる. 特に単位元は恒等的に 1 である指標 χ_0 (単位指標) で与えられる. (これも読者の練習問題としておこう.)

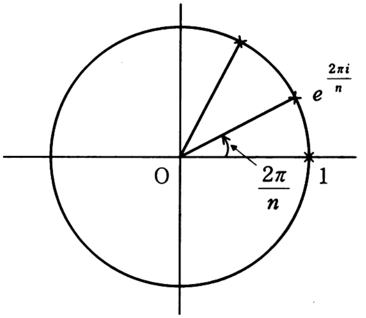
さて, 特に G が n 位の巡回群 $\langle a\rangle$ である場合を考えよう. $\chi \in \widehat{G}$ とすれば, $x = a^k$ に対して

$$\chi(x) = \chi(a^k) = \chi(a)^k$$

であるから, χ は $\chi(a)$ によって完全に決まる. $a^n = e$ であるから

$$\chi(a)^n = \chi(a^n) = \chi(e) = 1.$$

したがって $\chi(a)$ は 1 の n 乗根である．



よく知られているように，複素数の範囲で方程式

$$X^n - 1 = 0$$

の根（それを“1 の n 乗根”という）は

$$e^{2\pi i \frac{k}{n}} = \cos\left(2\pi \frac{k}{n}\right) + i \sin\left(2\pi \frac{k}{n}\right)$$

$$(\ k = 0, 1, \cdots, n-1\ ),$$

で与えられる．よって，$\chi \in \widehat{G}$ に対して，ある $k \in \boldsymbol{Z}$, $0 \leqq k \leqq n-1$ が定まり

$$\chi(a) = e^{2\pi i \frac{k}{n}}$$

となる．このとき $\chi = \chi_k$ とかくことにする．したがって，

$$\chi_k(a^l) = e^{2\pi i \frac{kl}{n}} \qquad (\ 0 \leqq l \leqq n-1\ ) \tag{5}$$

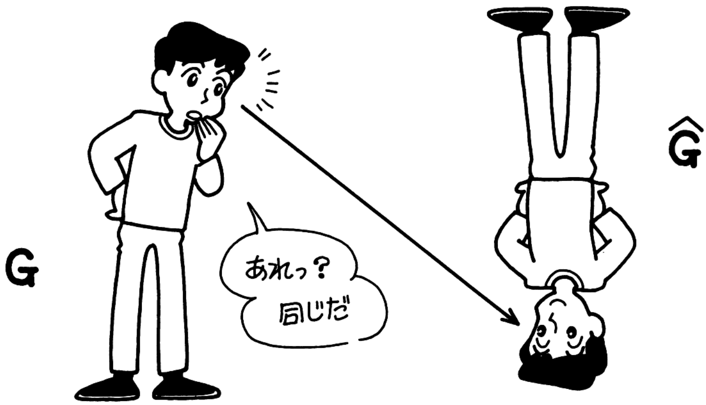
である．逆に，任意の $k \in \boldsymbol{Z}$, $0 \leqq k \leqq n-1$ に対して χ_k を (5) によって定義すれば，χ_k が G の指標になること（すなわち (3) が成立すること）は容易に確かめられる．

以上により

$$\widehat{G} = \{\ \chi_k\ (\ 0 \leqq k \leqq n-1\ )\ \} \tag{6}$$

であることがわかった．明らかに（$\widehat{G}$ における乗法の意味で）$\chi_k = (\chi_1)^k$ であるから，$\widehat{G}$ も χ_1 によって生成される n 位巡回群である．結論として，

定理 4.　G が n 位巡回群ならば，その指標群 $\hat{G}$ も n 位巡回群である．



G の自己双対性

3.3. 巡回群の双対性.　定理4によれば，n 位巡回群 G からその指標群 $\hat{G}$ を作れば，$\hat{G}$ もまた n 位巡回群になる．それならば，$\hat{G}$ の指標群 $\hat{\hat{G}}$ もまた n 位巡回群であるが，それはどのようなものであろうか．

上の議論において至るところ G を $\hat{G}$ でおきかえれば，$\hat{G}$ の代わりに $\hat{\hat{G}}$ がえられる．したがって

$$\hat{\hat{G}} = \{\varphi_l\ (0 \leqq l \leqq n-1)\}.$$

ここに，φ_l は

(7)
$$\varphi_l(\chi_1^k) = e^{2\pi i \frac{kl}{n}}$$

によって定義される $\hat{G}$ の指標である．$\chi_1^k = \chi_k$ であるから，(7) と (5) を比べれば，

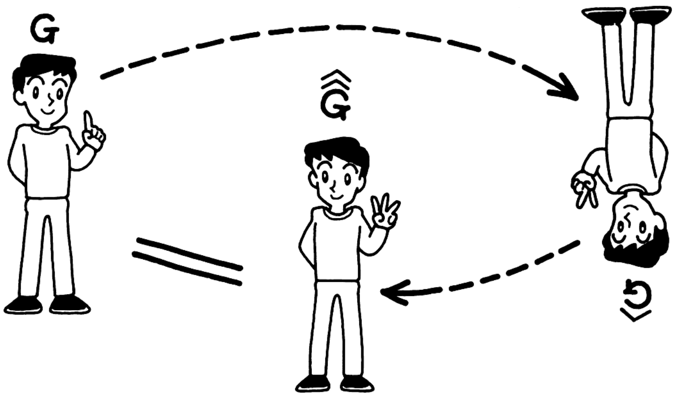
$$\varphi_l(\chi_k) = \chi_k(a^l).$$

すなわち，φ_l は χ_k に “a^l を代入する” という操作でえられる $\hat{G}$ の指標に他ならない．

G も $\hat{\hat{G}}$ もともに n 位の巡回群であるから，この対応

(8)
$$a^l \longleftrightarrow \varphi_l$$

（すなわち，a^l に，a^l を代入することによってえられる指標 φ_l を対応させる対応）は同型 $G \cong \hat{\hat{G}}$ を与える．しかも上の説明からわかるように，この同型対応は生成元 a のとり方に関係なく，自然な，標準的な対応として，ただ一通りに定まる．このように二つの群の間に自然な（canonical な）同型が存在するとき，数学ではそれら二つの群を同一視して（同じものとみなして）しまうことが多い．いまの場合，G と $\hat{\hat{G}}$ とは上の対応で同一視する（すなわち $a^l = \varphi_l$ と考える）ことができるのである．



このようにみるならば，$\chi_k(a^l)$ を考えるとき，これを写像

$$G \ni a^l \longmapsto \chi_k(a^l) \in \boldsymbol{C}^{(1)}$$

とみたものが指標 χ_k であり，写像

$$\hat{G} \ni \chi_k \longmapsto \chi_k(a^l) \in \boldsymbol{C}^{(1)}$$

とみたものが $\hat{G}$ の指標 φ_l（すなわち，a^l を代入するという指標）なのである．このように $\chi_k(a^l)$ における χ_k と a^l とは全く同格であるから，それを同等に取り扱って，$\langle \chi_k, a^l \rangle$ のように内積の形にかくこともある．すなわち

$$\chi_k(a^l) = \varphi_l(\chi_k) = \langle \chi_k, a^l \rangle. \tag{9}$$

結論として，$\hat{\hat{G}} = G$，すなわち G の双対の双対はそれ自身であるということができる．

3.4. 部分群の対応.　G の部分群 H に対し

$$H^{\perp} = \{ \chi \in \widehat{G} \mid \chi(h) = 1 \text{ for } \forall h \in H \}$$

とおけば，$H^{\perp}$ は $\widehat{G}$ の部分群になる．同様に，$\widehat{G}$ の部分群 Y に対し

$$Y^{\perp} = \{ x \in G \mid \eta(x) = 1 \text{ for } \forall \eta \in Y \}$$

とおけば，$Y^{\perp}$ は G の部分群になる．これらをそれぞれ H, Y の（$\widehat{G}, \widehat{\widehat{G}} = G$ における）"零化部分群"（annihilator）という．これらは線形代数における直交部分空間の類似物である．（そもそも指標群は双対空間のアナロジーである．）

さて H を n 位巡回群 G の一つの部分群とし，$|H| = l$ とおく．ラグランジュの定理により，l は n の約数である．（記号で $l|n$ とかく．）いま $x = a^k \in H$ とすれば，x の位数 $\operatorname{ord} x$ は l の約数であるから，

$$x^l = a^{kl} = e$$

この関係が成立するためには $n|kl$，すなわち $\dfrac{n}{l}|k$ が必要十分．よって $x \in \langle a^{n/l} \rangle$，したがって $H \subset \langle a^{n/l} \rangle$ である．しかし一方

$$\langle a^{\frac{n}{l}} \rangle = \{ e, a^{\frac{n}{l}}, a^{2\frac{n}{l}}, \cdots, a^{(l-1)\frac{n}{l}} \}$$

であるから，$|\langle a^{n/l} \rangle| = l$．したがって，上式で等号が成立し，$H = \langle a^{n/l} \rangle$ となることがわかる．

以上により，$l|n$ とするとき，G の部分群 H に対する次の三つの条件が同値であることがわかった．

1）$|H| = l$,

2）$H = \{ x \in G \mid x^l = e \}$,

3）$H = \langle a^{n/l} \rangle$.

一方，明らかに $x = a^k \in G$ に対して

$$x^l = e \iff \chi_l(x) = e^{2\pi i \frac{kl}{n}} = 1$$

であるから，上の条件 2) をみたす部分群 H は

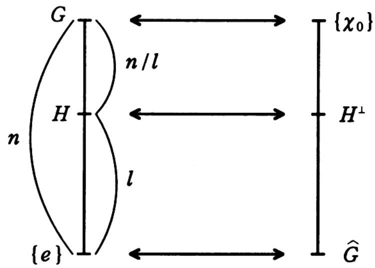
$$H = \langle \chi_l \rangle^{\perp}$$

として与えられることがわかる．以上により，次の定理がえられる．

定理 5. $G=\langle a \rangle$ を n 位の巡回群とすれば，G の部分群 H も巡回群である．n の約数 l に対して，位数 l の部分群 H はただ一つ存在し，

$$H = \langle a^{\frac{n}{l}} \rangle = \langle \chi_l \rangle^{\perp} \tag{10}$$

によって与えられる．



部分群の対応

上の定理において $\langle \chi_l \rangle$ は $\hat{G}$ の位数 n/l の部分群であり，H はその零化部分群である．定理5を $\hat{G}$ に適用すれば，$\hat{G}$ の位数 n/l の部分群もただ一つ定まる．それを Y とかけば，Y は巡回群 $\langle \chi_l \rangle$ に他ならない．それはまた $G=\hat{\hat{G}}$ の $n/(n/l)=l$ 位の部分群，すなわち H，の零化部分群になっている：$Y=H^{\perp}$.

このように，G の部分群と $\hat{G}$ の部分群とは $H=Y^{\perp}$，$Y=H^{\perp}$ という一種の直交関係で一対一に対応していることがわかる．したがって

$$Y^{\perp\perp} = H^{\perp} = Y, \qquad H^{\perp\perp} = Y^{\perp} = H$$

である．

例として，6 位の巡回群

$$G = \langle a \rangle = \{ e, a, a^2, a^3, a^4, a^5 \}$$

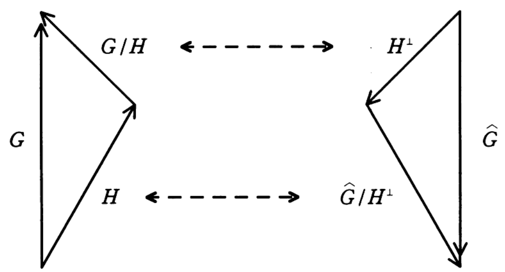
の部分群とその零化部分群の表を作ってみよう．

$H\ (\subset G)$	$H^{\perp}\ (\subset \widehat{G})$
$\{e, a, a^2, a^3, a^4, a^5\}$	$\{\chi_0\}$
$\{e, a^2, a^4\}$	$\{\chi_0, \chi_3\}$
$\{e, a^3\}$	$\{\chi_0, \chi_2, \chi_4\}$
$\{e\}$	$\{\chi_0, \chi_1, \chi_2, \chi_3, \chi_4, \chi_5\}$

H を G の部分群とするとき，H, G/H の指標群と G のそれとの間には次の関係（canonical な同型）が成立する．

(11) $$\widehat{H} \cong \widehat{G}/H^{\perp},$$

(12) $$\widehat{G/H} \cong H^{\perp}.$$



部分群，商群の双対関係

（証明）$\chi \in \widehat{G}$ に対して，その H への制限 $\chi|H$ を対応させる写像

$$\varphi : \chi \longmapsto \chi|H$$

を考える．$\varphi(\chi) = \chi|H$ は明らかに H の指標であり，

$$\varphi(\chi\chi') = \chi\chi'|H = \chi|H \cdot \chi'|H = \varphi(\chi)\varphi(\chi')$$

であるから，φ は $\widehat{G}$ から $\widehat{H}$ への準同型である．$\mathrm{Ker}\,\varphi$ は

$$\chi \in \mathrm{Ker}\,\varphi \iff \varphi(\chi) = \chi|H = 1$$
$$\iff \chi \in H^{\perp}$$

により，$\mathrm{Ker}\,\varphi = H^{\perp}$ である．よって，準同型定理により

(＊) $$\widehat{G}/H^{\perp} \cong \mathrm{Im}\,\varphi.$$

ここで $|H| = l$ とすれば，定理5により $|H^{\perp}| = n/l$ であるから，$|\mathrm{Im}\,\varphi| = l$.

一方，$|\widehat{H}| = |H| = l$ であるから，$\operatorname{Im}\varphi = \widehat{H}$ でなければならない．よって，(＊) から (11) がえられる．

(12) の証明も同様にしてできる．しかし，次のようにして (12) を (11) から導くこともできる．(11) において G, H をそれぞれ $\widehat{G}$, $H^{\perp}$ でおきかえれば，$\widehat{H}$ は $\widehat{H^{\perp}}$ でおきかえられる．よって

$$G/H = \widehat{\widehat{G}}/H^{\perp\perp} \cong \widehat{H^{\perp}}.$$

両辺の ^ をとれば，

$$\widehat{G/H} \cong \widehat{\widehat{H^{\perp}}} \cong H^{\perp}. \qquad \text{(証終)}$$

3.5. A氏らの不満.

またここで，A氏らの不満を聞いてみることにしよう．

＊　＊　＊

A氏 「わしにはまたまたよくわからない．なぜ急に指標群などというものを持ち出さなくてはならないのか？ 群 G があれば，それに付随していろいろな群が考えられるということはわかる．しかし，なぜ指標群 $\widehat{G}$ なのか？ そこのところを説明してもらわないと，わしにはどうもピンとこないのだ.」

C君 「G が巡回群ならば，$\widehat{G}$ も巡回群になる．G と $\widehat{G}$，同じ構造をもつ群を二つ並べてみてもあまり意味があるとは思えない．G と $\widehat{G}$ とは同型なのだから同一視してしまってもよいのじゃないかなぁ.」

Bさん 「でもそれは canonical ではないからダメよ.」

C君 「エ？」

Bさん 「G と $\widehat{\widehat{G}}$ とは canonical に同型だけれども，G と $\widehat{G}$ とはただ同型というだけで自然な対応がつかないの．そこがすごく違うのよ.」

C君 「ヘエー」

Bさん 「それに G と $\widehat{G}$ とを組にして考えると (一つだけ考えているより) 部分群の様子など立体的によく見えてくるような気がするわ．でも私もなぜ指標群を考えるのかと言われると，その必然性はよくわからない．な

ぜなんでしょう？」

＊　＊　＊

この話には二つのポイントがある．一つは canonical な同型とそうでないものの区別．もう一つはなぜ指標群を考えるかということ．最初の canonical な同型については，説明は簡単だと思う．

たとえば，G と $\widehat{G}$ との自然な同型対応をつけたいとする．簡単のため $n=6$ として考えることにしよう．

$$G = \langle a \rangle = \{ e, a, a^2, a^3, a^4, a^5 \},$$

$$\widehat{G} = \langle \chi_1 \rangle = \{ \chi_0, \chi_1, \chi_1^2, \chi_1^3, \chi_1^4, \chi_1^5 \}$$

であるから，一つの方法として

(＊)　$$a^k \longleftrightarrow \chi_1^k \qquad (k = 0, 1, 2, 3, 4, 5)$$

という対応を考えることができる．これは確かに G と $\widehat{G}$ の一つの同型対応を与える．しかし，この対応は $G, \widehat{G}$ の生成元 a, χ_1 のとり方に依存している．(数学者はこういうことに神経質なのです.) もしも G の生成元 a を固定して (つまり同型 $G \cong \boldsymbol{Z}/n\boldsymbol{Z}$ を固定して) 議論するというのであれば，これは canonical になる．しかし，一般には生成元のとり方は自由だと考える．いまの例でいえば，G は a の代わりに $b = a^5$ によっても生成される．実際，

$$b^0 = e, \quad b^1 = a^5, \quad b^2 = a^{10} = a^4, \quad b^3 = a^{15} = a^3,$$

$$b^4 = a^{20} = a^2, \quad b^5 = a^{25} = a$$

であるから

$$G = \{ e, b, b^2, b^3, b^4, b^5 \} = \langle b \rangle.$$

同様に，$\widehat{G}$ は χ_1 の代わりに $\chi_1^5 = \chi_5$ によっても生成される．したがって，上の対応の代わりに

$$b^k \longleftrightarrow \chi_1^k \qquad (k = 0, 1, 2, 3, 4, 5),$$

$$a^k \longleftrightarrow \chi_5^k \qquad (k = 0, 1, 2, 3, 4, 5),$$

$$b^k \longleftrightarrow \chi_5^k \qquad (k = 0, 1, 2, 3, 4, 5)$$

という対応を考えても一向に差し支えはないわけです．(賢明な読者は気がつ

かれたかもしれませんが，実は上述の第1の対応（＊）とこの第4の対応は同じものになり，また第2の対応と第3の対応も同じものになります.）しかし少なくとも第1の対応と第2の対応とは違うもので，一般にそのどちらがより自然なものかなどということは，われわれ（公平な心をもった数学者）には決めることが不可能なのです.

なにたった二つの同型ならどちらを選んでも大した違いはないなどと言ってはいけません. $n=6$ だから二つの同型しかでてきませんでしたが，たとえば $n=600$ とすれば，G は 160 個の相異なる生成元をもち，したがって，160 個の相異なる同型対応が生じることになります.

第二の，なぜ指標群を考えるかということはそう簡単には説明できません. 強いていえば，こういうことになる. つまり抽象的な群を考えるとき，一つの基本的な方法として，その群をより具体的な群と結びつけて考えるというやり方があります. そこで具体的な群としてまず考えられるのは，行列の群 $M_2(\boldsymbol{R})$, $GL_2(\boldsymbol{R})$ などです. これらは2次の行列の群ですが，それよりも簡単なのは1次の行列の群 $M_1(\boldsymbol{R})=\boldsymbol{R}$（$\boldsymbol{R}$ の加法群），$GL_1(\boldsymbol{R})=\boldsymbol{R}^\times$（$\boldsymbol{R}$ の乗法群）などです. ここで $\boldsymbol{R}$ を $\boldsymbol{C}$ でおきかえ，さらにそれを絶対値1の複素数の作る部分群 $\boldsymbol{C}^{(1)}$ でおきかえて，この群への準同型を考えたものが指標なのです.

一般に群 G から行列群 $GL_2(\boldsymbol{R})$, $GL_2(\boldsymbol{C})$ などへの準同型を G の（2次の）**表現**といいますが，指標は（1次の）表現の特別なもの（いわゆるユニタリーなもの）だということができます. 要するに，群 G を具体的な群 $\boldsymbol{C}^{(1)}$ と結びつけて考えようという思想から生まれたものなのです.

3.6. 直交関係式.

群 G に対して，なぜその双対 $\widehat{G}$ を考えるのか？ その理由の一つは，$\widehat{G}$ の元が G の上の"関数"であり，関数については乗法ばかりでなく加法も，さらには解析学のいろいろな演算を施すことも可能になるという利点があるのです.

いままで通り，巡回群 $G=\langle a\rangle$ とその双対 $\widehat{G}=\{\chi_k\}$ を考え，$|G|=|\widehat{G}|$

$=n$ とする.

χ_k $(0 \leqq k \leqq n-1)$ は G 上の関数であるから，まずその（関数としての）和が考えられる.

$$S(x) = \sum_{k=0}^{n-1} \chi_k(x) \qquad (x \in G)$$

とおく．ここで $x = a^l$ $(0 \leqq l \leqq n-1)$ を代入すれば,

$$S(a^l) = \sum_{k=0}^{n-1} e^{2\pi i \frac{kl}{n}}$$

となる．一番簡単な $x=e$，すなわち $l=0$ の場合には，明らかに

$$S(e) = 1 + \cdots + 1 = n$$

がえられる．$x \neq e$ の場合，$\mathrm{ord}\, x = m$ (>1)，$\zeta = e^{2\pi i l/n}$ とおけば，ζ は 1 の m 乗根で,

$$S(x) = \frac{n}{m}(1 + \zeta + \zeta^2 + \cdots + \zeta^{m-1})$$

となる．ζ は 1 の “原始 m 乗根”（すなわち m 乗してはじめて 1 になる数）であるから，上式の右辺の括弧の中は（根と係数の関係から）

$$X^m - 1 = \prod_{i=0}^{m-1}(X - \zeta^i)$$

の X^{m-1} の係数の（-1）倍と一致し，したがって $=0$．以上により

$$\text{(13)} \qquad \sum_{k=0}^{n-1} \chi_k(x) = \begin{cases} n & x = e \text{ のとき} \\ 0 & x \neq e \text{ のとき} \end{cases}$$

という簡単な公式がえられる.

上の結果は，次のようにもっと上手に証明することもできる.

$x=e$ のとき，$S(x)=n$ は明白だから，$x \neq e$ とする．そのときある $\eta \in \hat{G}$ があって $\eta(x) \neq 1$．（実際，$\chi_1(x) \neq 1$ である．）さて

$$\eta(x) S(x) = \sum_{k=0}^{n-1} \eta(x) \chi_k(x) = \sum_{k=0}^{n-1} (\eta \chi_k)(x).$$

χ_k が $\hat{G}$ のすべての元を動くとき，$\eta\chi_k$ も $\hat{G}$ のすべての元を動くから，上式

の右辺は $=S(x)$. すなわち

$$\eta(x)S(x) = S(x).$$

よって

$$(\eta(x)-1)S(x) = 0.$$

$\eta(x) \neq 1$ であるから,

$$S(x) = 0$$

でなければならない. (証終)

G と $\hat{G}$ の双対性により

(14) $$\sum_{x \in G} \chi(x) = \begin{cases} n & \chi = \chi_0 \text{ のとき} \\ 0 & \chi \neq \chi_0 \text{ のとき} \end{cases}$$

も成立する. (13), (14) は指標の **直交関係式** と呼ばれている.

3.7. フーリエ変換.

G 上の任意の(複素)関数 $f(x)$ に対し

(15) $$\hat{f}(\chi) = \sqrt{n}^{-1} \sum_{x \in G} f(x)\chi(x)$$

によって f の **フーリエ** (Fourier) **変換** $\hat{f}$ を定義する. $\hat{f}$ は指標群 $\hat{G}$ 上の(複素)関数である.

定理 6. フーリエ変換に関して, 次の等式が成立する. (H は G の任意の部分群とする.)

(16) $$|H^{\perp}|^{-\frac{1}{2}} \sum_{\chi \in H^{\perp}} \hat{f}(\chi) = |H|^{-\frac{1}{2}} \sum_{x \in H} f(x)$$

(17) $$\hat{\hat{f}}(x) = f(x^{-1}).$$

((16) は **ポアソン** (Poisson) **の和公式** と呼ばれている.)

(証明) これらは簡単な計算で確かめられる. 定義により

(＊) $$\sum_{\chi \in H^{\perp}} \hat{f}(\chi) = \sqrt{n}^{-1} \sum_{\chi \in H^{\perp}} \sum_{x \in G} f(x)\chi(x)$$
$$= \sqrt{n}^{-1} \sum_{x \in G} f(x) \left(\sum_{\chi \in H^{\perp}} \chi(x) \right).$$

ここで（12）により $H^{\perp}=\widehat{G/H}$ とみなせることから，（13）により

$$\sum_{\chi\in H^{\perp}}\chi(x)=\begin{cases}|H^{\perp}| & x\in H\text{ のとき}\\ 0 & x\notin H\text{ のとき}\end{cases}$$

となる．ラグランジュの定理により，$n=[G:H]\cdot|H|=|H^{\perp}|\cdot|H|$ であるから，（＊）の右辺は

$$=(|H^{\perp}|/|H|)^{\frac{1}{2}}\sum_{x\in H}f(x).$$

（17）の証明：

$$\begin{aligned}\hat{\hat{f}}(y)&=\frac{1}{n}\sum_{\chi\in\widehat{G}}\sum_{x\in G}f(x)\chi(x)\chi(y)\\&=\frac{1}{n}\sum_{x\in G}f(x)\Bigl(\sum_{\chi\in\widehat{G}}\chi(xy)\Bigr)\end{aligned}$$

ここで（13）により

$$\sum_{\chi\in\widehat{G}}\chi(xy)=\begin{cases}n & xy=e,\text{ i.e. }x=y^{-1}\text{ のとき}\\ 0 & xy\neq e\text{ のとき}.\end{cases}$$

よって

$$\hat{\hat{f}}(y)=f(y^{-1}).\qquad\text{（証終）}$$

式（15）において，なぜ $\sqrt{n}^{-1}$ をつけるのか疑問に思う読者がいると思う．$\sqrt{n}^{-1}$ をつけずに $\hat{f}$ を定義することも可能であるが，そうすると（17）の式は $\hat{\hat{f}}(x)=nf(x^{-1})$ となり，フーリエ変換を2回施すともとに戻るという直感に合わなくなる．これは元来“測度”（measure）の問題であって，G にどのような測度を導入するのが自然かという問題に関係している．G は n 個の点からなる集合であるから，各点が測度1をもつと考えれば，G 全体の測度は n になる．しかし G はコンパクトだから，G の全測度は1であると考えるのも自然な考え方で，そのとき各点の測度は $1/n$ になる．そこで，この二つの平均をとって各点の測度を $\sqrt{n}^{-1}$ とするのが合理的ということになる．これは G をその自己双対性に適した測度で考えることに他ならない．式（16）の

両辺に $|H^\perp|^{-1/2}$ や $|H|^{-1/2}$ が現れるのも同じ理由によるのである.

3.8. ガウスの和. ここでちょうどよい機会なので，巡回群の双対性の一つの応用として，ガウスの和について説明する．p を奇素数，$G=\boldsymbol{Z}/p\boldsymbol{Z}$ とし，(canonical な) 対応

$$G \ni y \longmapsto \chi_y \in \widehat{G},$$
(18)
$$\chi_y(x) = e^{2\pi i \frac{xy}{p}}$$

によって G をその双対 $\widehat{G}$ と同一視して考えることにする.

(18) 第2式の右辺は便宜的な書き方である．すなわち，$x, y \in G$ は $\bmod p\boldsymbol{Z}$ の剰余類であるが，その（$\boldsymbol{Z}$ における）代表元 x_1, y_1 をとり，$e^{2\pi i x_1 y_1/p}$ を考えると，これは代表 x_1, y_1 のえらび方に関係なく定まる．それを $e^{2\pi i xy/p}$ とかくのである．以下においても同じように，G 上の関数と $\boldsymbol{Z}$ 上の周期 p をもつ関数とを同一視して同じ記号で表すことが多い.

G 上の関数 $f(x)$ を次のように定義する.

$$f(x) = \begin{cases} 0 & x=[0] \text{ のとき} \\ 1 & \exists y \neq [0],\ x=y^2 \text{ のとき} \\ -1 & \text{そうでないとき}. \end{cases} \tag{19}$$

ただし [0] は，$G=\boldsymbol{Z}/p\boldsymbol{Z}$ におけるゼロ，すなわち剰余類 $p\boldsymbol{Z}$ を表す．$f(x)$ は p を法とする（ルジャンドルの）“平方剰余記号”と呼ばれ，普通 $\left(\dfrac{x}{p}\right)$ とかかれる．この関数について，明らかに

$$f(xy) = f(x)f(y)$$

が成立する．すなわち，$f(x)$ ($x \neq [0]$) は（乗法群 $(\boldsymbol{Z}/p\boldsymbol{Z})^\times$ の）指標である.

$f(x)$ のフーリエ変換は，定義により

$$\widehat{f}(y) = \sqrt{p}^{\,-1}\sum_{x=0}^{p-1} f(x)e^{2\pi i \frac{xy}{p}} \tag{20}$$

となる．いま $z\in G$, $z\neq[0]$ とし，(20) において x を xz でおきかえれば，



ゲッチンゲン市，Neues Rathaus の近くにあるガウス-ウェーバー記念像（ガウスは物理学者 W. Weber と協力して電磁気学の研究にもたずさわった.）

$f(xz)=f(x)f(z)$ であるから，

$$\hat{f}(y) = f(z)\hat{f}(zy)$$

という関係式がえられる．$y \neq [0]$ のとき，$z=y^{-1}$ とおけば，$f(y^{-1})=f(y)$ であるから

$$\hat{f}(y) = f(y)\hat{f}(1) \tag{21}$$

となる．よって $\eta=\hat{f}(1)$ とおけば，$\hat{f}(y)=\eta f(y)$，すなわち $f(x)$ はそのフーリエ変換 $\hat{f}(x)$ と定数倍を除いて一致することがわかる．

（21）により

$$\hat{\hat{f}}(x) = \eta\hat{f}(x) = \eta^2 f(x).$$

一方，（17）により

$$\hat{\hat{f}}(x) = f(-x) = f(-1)f(x)$$

であるから（$f(x)$ が恒等的には 0 でないことにより），

$$\eta^2 = f(-1) \tag{22}$$

がえられる.

$$\gamma = \eta\sqrt{p} = \sum_{x=0}^{p-1} f(x) e^{2\pi i \frac{x}{p}}$$

を**ガウス**（Gauss）**の和*** という. 上の（22）により

$$\gamma^2 = \left(\frac{-1}{p}\right)p \tag{23}$$

である.（さらに $\eta = 1$ または i となることが証明される.* しかしそのためにはより精密な議論が必要である.）

3.9. 一般のアーベル群の場合. いままで簡単のため巡回群について説明してきたが, 実は上に述べたと同じことが一般の有限アーベル群（可換群）についても成り立つことが知られている.* その証明は, 2.13 節で述べた有限アーベル群の基本定理によって, 巡回群の場合に帰着される.

G を一般に有限アーベル群とし, その指標群（双対）$\hat{G}$ を上と同様 G の指標（G から $\boldsymbol{C}^{(1)}$ への準同型）全体の作る群として定義する. そのとき次のことがいえる.

1. 群として（一般には non-canonical に）$\hat{G} \cong G$ である. 特に $|\hat{G}| = |G|$.
2. G と $\hat{\hat{G}}$ は, $a \in G$ に $\varphi_a \in \hat{\hat{G}}$,
$$\varphi_a(\chi) = \chi(a) \qquad (\chi \in \hat{G}),$$
を対応させる写像 $a \mapsto \varphi_a$ によって canonical に同型である.
3. $G, \hat{G}$ の部分群 H, Y に対し, その零化部分群 $H^\perp$, $Y^\perp$ を 3.4 におけると同じ式で定義すれば, それらはそれぞれ $\hat{G}, G$ の部分群で, 互いに逆な対応
$$H \longmapsto H^\perp, \qquad Y \longmapsto Y^\perp$$
により G の部分群と $\hat{G}$ の部分群とは一対一に対応する.（したがって $H^{\perp\perp} = H$, $Y^{\perp\perp} = Y$.）対応する部分群の位数について等式

$$(\ast)\qquad |H|\cdot|H^{\perp}| = |Y|\cdot|Y^{\perp}| = n$$

が成立する．また自然な同型

$$\widehat{H} \cong \widehat{G}/H^{\perp},\qquad \widehat{G/H} \cong H^{\perp}$$

が成立する．

さらに指標の直交関係式 (13), (14) も一般に成立する．（第二の証明がそのまま適用される．）フーリエ変換の公式 (15), (16), (17) もそのまま成立する．

これらの関係はさらに位相アーベル群の場合に拡張される.* すなわち位相アーベル群の中で，局所コンパクトであるもの G に対し，その“双対”（指標群）$\widehat{G}$ を G の連続な指標全体に適当な位相を導入したものと定義すれば，$\widehat{G}$ も局所コンパクト位相アーベル群になる．この局所コンパクト位相アーベル群の範囲で“双対性”（上記2の性質）が成立する．また $G, \widehat{G}$ の部分群 H, Y として閉部分群のみを考えることにすれば，部分群の対応（上記3の性質）も（位数の関係式（$\ast$）を除いて）そのまま成立する．

さらに，フーリエ変換の公式 (15), (16), (17) 等も一般の局所コンパクトアーベル群に対して（和を適当な無限和または積分でおきかえることにより，適当な収束条件の下に）成立する．

しかし，上記1の性質は必ずしも成立しない．この性質が成立するとき局所コンパクトアーベル群 G は“自己双対的”であるという．上記によれば，有限アーベル群は（離散的な位相をもつ位相アーベル群として）自己双対的である．また，$G=\boldsymbol{R}^n$（n 次元ベクトル群）は自然な位相に関して局所コンパクト位相アーベル群になり，$\widehat{G}\cong\boldsymbol{R}^n$ である．すなわち，$G=\boldsymbol{R}^n$ も自己双対的である．また，G の双対 $\widehat{G}$ はそのベクトル空間としての双対空間と一致する．このように，有限次元ベクトル空間の双対性は，局所コンパクト位相アーベル群の双対性の特別な場合とみることができる．

一般の局所コンパクトアーベル群の双対性は，“ポントリャーギン (Pontrjagin) の双対性”と呼ばれている．前にあげたガウスの和の例や次

に説明するテータ関数の例からもわかるように，位相アーベル群の双対性は整数論においてきわめて重要な意味をもっている．

3.10. テータ関数の関数等式. 位相アーベル群の双対性の一つの応用例として，有名なテータ関数の関数等式（反転公式）を導いてみよう．

考える群は $G=\boldsymbol{R}$ (実数の加群)，もちろん位相群としての $\boldsymbol{R}$ である．$y\in\boldsymbol{R}$ に対し

$$\chi_y(x) = e^{2\pi ixy} \qquad (x\in\boldsymbol{R})$$

とおけば，これが（x の関数として）G の連続な指標を与えることは見やすい．しかも，G の連続指標はすべてこの形でえられることが証明される．いいかえれば，写像

$$y\,(\in G\,) \longmapsto \chi_y\,(\in \widehat{G}\,)$$

は同型 $G\cong\widehat{G}$ を与える．これが $G=\boldsymbol{R}$ の自己双対性である．この同型も canonical であるから，それを同一視して $G=\widehat{G}=\boldsymbol{R}$ と考えることにする．そのとき，$\boldsymbol{Z}$ は $\boldsymbol{R}$ の離散部分群であるが，その零化部分群は（すぐわかるように）$\boldsymbol{Z}$ 自身である．この場合，$H=H^{\perp}=\boldsymbol{Z}$ に関する公式（16）は

$$\sum_{n=-\infty}^{\infty} f(n) = \sum_{n=-\infty}^{\infty} \widehat{f}\,(n) \tag{24}$$

の形になる．これが本来の“ポアソンの和公式”である．

さて，$\boldsymbol{R}$ 上の（複素）関数 $f(x)$ に対してそのフーリエ変換 $\widehat{f}\,(y)$ は，定義により

$$\widehat{f}\,(y) = \int_{-\infty}^{\infty} f(x)\,e^{2\pi ixy}\,dx \tag{25}$$

である．上述のように，（$f(x)$ に関する）適当な条件の下にこの積分は収束し，さらに（24）の両辺の無限和も収束して相等しいことが知られている．ここでその条件については述べない．（これについては位相群の教科書，たとえば [W]，および [Sc] 参照.） われわれにとっては，特別な一つの関数

(26) $$f(x) = e^{-x^2}$$

がこの条件をみたすことを認めるだけで十分である．（e^{-x^2} は C^∞ 急減少関数で，このような関数は上述の条件をみたすことが知られている．）

簡単な計算により

$$\hat{f}(y) = \int_{-\infty}^{\infty} \exp(-x^2 + 2\pi ixy)\,dx$$
$$= \int_{-\infty}^{\infty} \exp(-(x-\pi iy)^2 - \pi^2 y^2)\,dx.$$

ここで

$$C = \int_{-\infty}^{\infty} \exp(-(x-\pi iy)^2)\,dx$$

は y に無関係な定数になる．よって

(27) $$\hat{f}(y) = Cf(\pi y)$$

である．

さて，実数部が正であるような複素数 α に対して

$$g(x) = f(\alpha x) = e^{-\alpha^2 x^2}$$

とおけば，$g(x)$ に対しても上述の条件が成立し，簡単な計算でわかるように

(28) $$\hat{g}(y) = \alpha^{-1}\hat{f}\left(\frac{y}{\alpha}\right)$$

となる．

(27), (28) により

$$\hat{\hat{f}}(x) = \frac{C}{\pi}\hat{f}\left(\frac{x}{\pi}\right) = \frac{C^2}{\pi}f(x).$$

一方，(17) により $\hat{\hat{f}}(x) = f(-x) = f(x)$ であるから，$C^2 = \pi$，$C = \sqrt{\pi}$ を得る．（これはガウスの和の計算とよく似ている！　もちろん，この結果は定積分の計算からも導かれる．）

さて $z = x+iy$, $y > 0$（すなわち，z は複素上半平面の点）とし，テータ関

数*

$$\theta(z) = \sum_{n=-\infty}^{\infty} e^{\pi i z n^2} \tag{29}$$

を考える．右辺の無限級数が上半平面で広義の一様に絶対収束することは，ただちにわかる．したがって，$\theta(z)$ は上半平面上の正則関数である．

$$\alpha = \sqrt{-\pi i z} = \sqrt{\pi(y-ix)}$$

を実数部が正であるような平方根の一つの枝を表すものとし，$g(t) = f(\alpha t)$ とおけば

$$\theta(z) = \sum_{n=-\infty}^{\infty} g(n)$$

と表される．上記により

$$\begin{aligned}\hat{g}(t) &= \alpha^{-1}\hat{f}\left(\frac{t}{\alpha}\right) = \frac{\sqrt{\pi}}{\alpha} f\left(\frac{\pi}{\alpha}t\right)\\ &= \frac{1}{\sqrt{-iz}}\exp(\pi i(-1/z)t^2)\end{aligned}$$

であるから

$$\sum_{n=-\infty}^{\infty} \hat{g}(n) = \frac{1}{\sqrt{-iz}}\theta\left(-\frac{1}{z}\right).$$

よって，ポアソンの和公式から θ の関数等式（反転公式）

$$\theta(z) = \frac{1}{\sqrt{-iz}}\theta\left(-\frac{1}{z}\right) \tag{30}$$

がえられる．これは θ が重さ 1/2 のモジュラー形式* になることを示す重要な公式である．

第4章　ちょっと変わったガロア理論

まず，第3章で述べた有限アーベル群 G とその双対 $\widehat{G}$ の部分群の対応を一般化することを試みる．その応用としてガロア理論を考える．

4.1．親密な関係．　$\mathscr{A}$, $\mathscr{X}$ を二つの集合とし，それぞれの元を $a, b, \cdots$; $x, y, \cdots$ 等とかく．また，$\mathscr{A}$, $\mathscr{X}$ の部分集合をそれぞれ $A, B, \cdots ; X, Y, \cdots$ とかく．

いま，直積集合 $\mathscr{A}\times\mathscr{X}$ の一つの部分集合 $\mathscr{R}$ が与えられたとする．$(a, x)\in\mathscr{R}$ であるとき，（たとえば）a と x とは親密な関係にあるということにしよう．

さて，$A\subset\mathscr{A}$, $X\subset\mathscr{X}$ に対し

$$\varphi(A) = \{x\in X \mid (a, x)\in\mathscr{R} \text{ for } \forall a\in A\},$$

$$\psi(X) = \{a\in A \mid (a, x)\in\mathscr{R} \text{ for } \forall x\in X\}$$

と定義する．φ は $\mathscr{A}$ の部分集合 A に対し，A のすべての元と親密な関係にある $\mathscr{X}$ の元全部の集合 $\varphi(A)$ を対応させる写像，ψ は逆に $\mathscr{X}$ の部分集合 X に，X のすべての元と親密な関係にある $\mathscr{A}$ の元全部の集合 $\psi(X)$ を対応させる写像である．（空集合に対しては $\varphi(\phi)=\mathscr{X}$, $\psi(\phi)=\mathscr{A}$ とおく．すべての人は幻の恋人と親密な関係にあるのである．）

$\mathscr{A}$ の部分集合 A から出発して，この操作をくりかえしてゆけば

$$A,\ \varphi(A),\ \psi(\varphi(A)),\ \varphi(\psi(\varphi(A))),\ \cdots$$

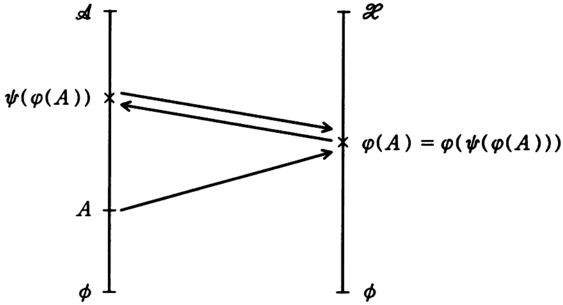
等々がえられる．このとき次のことは，いずれも定義から明白であろう．

(1) $$A \subset \psi(\varphi(A)),$$

(2) $$A \subset B \implies \varphi(A) \supset \varphi(B),$$

(3) $$\varphi\Bigl(\bigcup_{\lambda \in \Lambda} A_\lambda\Bigr) = \bigcap_{\lambda \in \Lambda} \varphi(A_\lambda).$$

（ここに Λ は有限または無限の添数の集合を表す.）



同様に

(1′) $$X \subset \varphi(\psi(X)),$$

(2′) $$X \subset Y \implies \psi(X) \supset \psi(Y),$$

(3′) $$\psi\Bigl(\bigcup_{\lambda \in \Lambda} X_\lambda\Bigr) = \bigcap_{\lambda \in \Lambda} \psi(X_\lambda)$$

も成立する.

定理 1. 任意の $A \subset \mathscr{A}$, $X \subset \mathscr{X}$ に対して，次の等式が成立する.

(4) $$\varphi(\psi(\varphi(A))) = \varphi(A),$$

(4′) $$\psi(\varphi(\psi(X))) = \psi(X).$$

（証明） (1), (2) から

$$\varphi(A) \supset \varphi(\psi(\varphi(A))).$$

一方，(1′) を $X = \varphi(A)$ に適用すれば，

$$\varphi(A) \subset \varphi(\psi(\varphi(A))).$$

よって，等式 (4) がえられる. (4′) についても同様である.　　（証終）

定理 2. $A \subset \mathscr{A}$ に対し，$\widetilde{A} = \psi(\varphi(A))$ とおけば，写像 $A \mapsto \widetilde{A}$ は次の性質をもつ.

(i)　$A \subset \widetilde{A}$,

(ii)　$\widetilde{\widetilde{A}} = \widetilde{A}$,

(iii)　$A \subset B \implies \widetilde{A} \subset \widetilde{B}$,

(iv)　$A = \bigcap_{\lambda \in \Lambda} A_\lambda,\ \widetilde{A}_\lambda = A_\lambda\ (\lambda \in \Lambda) \implies \widetilde{A} = A$.

これらも上に述べたことから明らかであろう．写像

$$X \longmapsto \widetilde{X} = \varphi(\psi(X))$$

についても同じことがいえる．一般に (i) − (iv) の性質をもつ写像を“閉演算”という．トポロジーにおいて，一つの位相空間 $\mathscr{X}$ の部分集合 X にその“閉包” $\overline{X}$ (X を含む最小の閉集合) を対応させる写像は明らかに一つの閉演算である．そこでトポロジーの言葉を流用して，一般に $A = \widetilde{A}$ となるとき，A を**閉集合**ということにする．

定理 3. $\mathscr{A}$ の閉集合と $\mathscr{X}$ の閉集合とは，互いに逆な写像 φ, ψ により一対一に対応する．

(証明)　$\mathscr{A}$ の閉集合 A に対し，$X = \varphi(A)$ とおけば (4) により

$$\widetilde{X} = \varphi(\psi(\varphi(A))) = \varphi(A) = X$$

であるから，X は $\mathscr{X}$ の閉集合である．また

$$\psi(X) = \psi(\varphi(A)) = \widetilde{A} = A$$

が成立する．同様に $\mathscr{X}$ の閉集合 X に対し，$A = \psi(X)$ とおけば，A は $\mathscr{A}$ の閉集合で $\varphi(A) = X$ である．よって，写像 φ, ψ は $\mathscr{A}, \mathscr{X}$ の閉集合の間の互いに逆な一対一対応を与える．　(証終)

例. 前章の例では

$$\mathscr{A} = G\ (\text{有限アーベル群}),$$

$$\mathscr{X} = \widehat{G}\ (\text{その指標群}),$$

$$\mathscr{R} = \{(a, \chi) \in G \times \widehat{G} \mid \chi(a) = 1\}$$

である．このとき次のことがいえる．

(S)　$A \subset G,\ Y \subset \widehat{G}$ が閉集合になるためには，A, Y が $G, \widehat{G}$ の部分群になる

ことが必要十分である.

実際，任意の $A \subset G, Y \subset \widehat{G}$ に対して

$$\varphi(A) = \{\chi \in \widehat{G} \mid \chi(a) = 1 \text{ for } \forall a \in A\},$$

$$\psi(Y) = \{a \in G \mid \chi(a) = 1 \text{ for } \forall \chi \in Y\}$$

は明らかに $\widehat{G}$, G の部分群になる.（空集合に対しては $\varphi(\phi) = \widehat{G}$, $\psi(\phi) = G$ であった.）よって閉集合は部分群である．逆に A が G の部分群ならば，

$$\varphi(A) = A^{\perp}, \qquad \psi(\varphi(A)) = A^{\perp\perp} = A$$

であるから A は閉集合である．$Y \subset \widehat{G}$ についても同様である．（証終）

4.2. 代数的数. まず基本的な二，三の概念の説明から始めることにする．

ブールバキの用法に従って，有理数全体の集合を $\boldsymbol{Q}$ で表す．$\boldsymbol{Q}$ の中で加減乗除の演算ができ，通常の演算法則が成立することはよく知られている．抽象代数の言葉でいえば，

（F1） $\boldsymbol{Q}$ は加法に関して可換群（加群）になる.

（F2） $\boldsymbol{Q}^{\times} = \boldsymbol{Q} - \{0\}$ は乗法に関して可換群になる.

（F3） 加法と乗法に関して分配律

$$a(b+c) = ab + ac$$

が成立する.

一般に（F1）-（F3）をみたす二つの演算が定義されている集合を（その演算もこめて）**体** という．実数全体の集合 $\boldsymbol{R}$，複素数全体の集合 $\boldsymbol{C}$ なども体である．そして（演算までこめて）$\boldsymbol{Q} \subset \boldsymbol{R} \subset \boldsymbol{C}$ である.

$\boldsymbol{Q}$ の元を係数とする多項式を

$$f(x) = \sum_{i=0}^{n} a_i x^i, \qquad a_i \in \boldsymbol{Q}$$

のようにかき表す．（$a_n \neq 0$ のとき，$f(x)$ は次数 n であるといい，$\deg f(x) = n$ とかく．0の次数は $-\infty$ であると定義する.）また，このような多項式全体の集合を $\boldsymbol{Q}[x]$ で表す．$\boldsymbol{Q}[x]$ においても加法と乗法とが定義されていて，

上記の（F1）－（F3）（ただし $\boldsymbol{Q}$ を $\boldsymbol{Q}[x]$ でおきかえる）のうち，（F2）において $\boldsymbol{Q}[x]-\{0\}$ の元に逆元が存在するということを除き，すべての条件が成立する．抽象代数ではこのような集合を（その演算もこめて）1 をもつ **可換環** という．有理整数全体の集合 $\boldsymbol{Z}$ も 1 をもつ可換環の例である．

一般に 1 をもつ可換環 R があるとき，$a \in R$ は，$ax=1$ となる $x \in R$ が存在するとき，R の“可逆元”であるという．R の可逆元全体が（乗法に関して）可換群になることは見やすい．（これも簡単な演習問題である．）R の可逆元全体の作る群を R の **単数群** といい，$R^{\times}$ で表す．たとえば

$$\boldsymbol{Z}^{\times} = \{\pm 1\}, \qquad \boldsymbol{Q}[x]^{\times} = \boldsymbol{Q}^{\times} = \boldsymbol{Q}-\{0\}$$

である．

さて $f(x) = \sum_{i=0}^{n} a_i x^i \in \boldsymbol{Q}[x]$ が与えられたとき，$\alpha \in \boldsymbol{C}$ に対し，

$$f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i \in \boldsymbol{C}$$

を $f(x)$ に α を代入した値，または $f(x)$ の“$x=\alpha$ における値”という．対応 $\alpha \mapsto f(\alpha)$ は一つの複素関数（“多項式関数”）を定義する．（それも同じ $f(x)$ で表す．）一方，$\alpha \in \boldsymbol{C}$ を固定し，写像

$$f(x)\ (\in \boldsymbol{Q}[x]) \longmapsto f(\alpha)\ (\in \boldsymbol{C})$$

を考えると，これは $\boldsymbol{Q}[x]$ から $\boldsymbol{C}$ への（可換）環の準同型になる．この準同型の核，すなわち

$$I(\alpha) = \{\, f(x) \in \boldsymbol{Q}[x] \mid f(\alpha)=0 \,\} \tag{5}$$

を α の“零化イデアル”（annihilator）という．（これは実際，可換環論の意味でのイデアルになる．）また $f(x) \neq 0$，$f(\alpha)=0$ であるとき，α は多項式 $f(x)$ の **零点** であるという．通常，言葉を乱用して α を $f(x)$ の根（最近では解）ということもある．（正確には α は方程式 $f(x)=0$ の根または解というべきであろう．）有理係数の（0でない）多項式 $f(x) \in \boldsymbol{Q}[x]$ の零点になるような複素数 α を **代数的数**，そうでない複素数を超越数という．

たとえば，$\alpha = 2+\sqrt{3}$ は多項式

$$f(x) = (x-2)^2 - 3 = x^2 - 4x + 1$$

の零点であるから代数的数である．しかし，e や π は代数的でない，すなわち超越的である．（その証明は難しい！）

4.3. ザリスキー位相.

ここでわれわれは手始めに次の組合せを考える．

$$\mathscr{A} = \boldsymbol{C},$$

$$\mathscr{X} = \boldsymbol{Q}[x],$$

$$\mathscr{R} = \{ (\alpha, f(x)) \in \boldsymbol{C} \times \boldsymbol{Q}[x] \mid f(\alpha) = 0 \}.$$

このとき $\mathscr{A}$, $\mathscr{X}$ における閉集合はどんなものになるだろうか？

まず $A \subset \mathscr{A} = \boldsymbol{C}$ に対して，定義により

$$\varphi(A) = \{ f(x) \in \boldsymbol{Q}[x] \mid f(\alpha) = 0 \text{ for } \forall \alpha \in A \}$$

であるから，

$$\varphi(A) = \bigcap_{\alpha \in A} I(\alpha) \tag{6}$$

である．これを A の零化イデアルという．

一般に，$\boldsymbol{Q}[x]$ の部分集合 J は条件

$$\text{(I)} \quad \begin{aligned} &f(x), g(x) \in J \implies f(x) + g(x) \in J, \\ &f(x) \in \boldsymbol{Q}[x],\ g(x) \in J \implies f(x)g(x) \in J \end{aligned}$$

をみたすとき，可換環 $\boldsymbol{Q}[x]$ の**イデアル**であるという．上記の $I(\alpha)$, $\varphi(A)$ 等は確かに $\boldsymbol{Q}[x]$ のイデアルになっている．いま $f_0(x) \in \boldsymbol{Q}[x]$ を一つとり，

$$J = \{ g(x)f_0(x) \mid g(x) \in \boldsymbol{Q}[x] \},$$

すなわち $f_0(x)$ の“倍数”（倍式？）全体の集合を J とすれば，J は明らかに一つのイデアルになる．これを $f_0(x)$ によって生成される単項イデアルといい，簡単のため $J = (f_0(x))$ とかく．また $f(x) \in (f_0(x))$ のとき，$f_0(x) \mid f(x)$ とかく．

ここで，次の（多分よくご存知の）定理が成立する．

定理 4. 可換環 $\boldsymbol{Q}[x]$ のイデアルはすべて単項イデアルである．

証明は簡単である．J を $\boldsymbol{Q}[x]$ の任意のイデアルとする．$J = \{0\}$ ならば，

$J=(0)$ であるから，J は単項である．よって $J\neq\{0\}$ と仮定してよい．そのとき J に含まれる 0 でない多項式のうち，次数が最小なものをとり $f_0(x)$ とする．任意の $f(x)\in J$ をとれば，ユークリッドのアルゴリズムにより

$$f(x) = q(x)f_0(x)+r(x),$$
$$q(x), r(x) \in \boldsymbol{Q}[x],\quad \deg r(x) < \deg f_0(x)$$

とかくことができる．$f(x), f_0(x)\in J$ であるから，条件（I）により

$$r(x) = f(x)-q(x)f_0(x) \in J.$$

よって $f_0(x)$ のとり方により，$r(x)=0$ でなければならない．すなわち，$f(x)=q(x)f_0(x)$ となる．逆に $f(x)$ がこの形ならば，（I）により $f(x)\in J$ である．よって $J=(f_0(x))$ である．（証終）

上の証明における $f_0(x)$ は一意的ではなく，$\boldsymbol{Q}[x]$ の単数倍を除いて決まる．すなわち，任意の $c\in\boldsymbol{Q}$, $c\neq 0$ に対し $f_0(x)$ を $cf_0(x)$ でおきかえてもよい．よって，$f_0(x)$ をその最高次の係数が 1 であるように正規化することができる．このように正規化された J の生成元を J の **最小多項式** ということにする．$J=I(\alpha)$ のとき，J の最小多項式を“α の最小多項式”ともいう．

一般に，$J=(f_0(x))\neq\{0\}$ であるとき，明らかに

$$\begin{aligned}\psi(J) &= \{\alpha\in\boldsymbol{C} \mid f(\alpha)=0 \text{ for } \forall f(x)\in J\}\\ &= \{\alpha\in\boldsymbol{C} \mid f_0(\alpha)=0\}\end{aligned}$$

すなわち，$\psi(J)$ は $f_0(x)$ の零点の集合に他ならない．よって，それは代数的数からなる有限集合で，その元の個数は $\deg f_0(x)$ をこえない．

さて，$\mathscr{A}=\boldsymbol{C}$, $\mathscr{X}=\boldsymbol{Q}[x]$ の閉集合を決定するために，まず $A=\phi$ の場合を考える．定義により

$$\varphi(\phi) = \mathscr{X},\qquad \psi(\varphi(\phi)) = \psi(\mathscr{X}) = \phi.$$

また，$A=\boldsymbol{C}$ とすれば

$$\varphi(\boldsymbol{C}) = (0),\qquad \psi(\varphi(\boldsymbol{C})) = \psi((0)) = \boldsymbol{C}.$$

よって

(7) $$\phi \longleftrightarrow \mathscr{X}=(1),\qquad \mathscr{A}=\boldsymbol{C}\longleftrightarrow(0)$$

は互いに対応する $\mathscr{A}=\boldsymbol{C}$ と $\mathscr{X}=\boldsymbol{Q}[x]$ の閉集合であることがわかる．

そこで，$A\subset\boldsymbol{C}$ を閉集合で，$A\neq\phi,\boldsymbol{C}$ とする．対応する $\mathscr{X}=\boldsymbol{Q}[x]$ の閉集合 $J=\varphi(A)$ は（上に述べたように）$\boldsymbol{Q}[x]$ のイデアルで，$J\neq(1),(0)$．よって，J の最小多項式 $f_0(x)$ は $\neq 1,0$ で，$A=\psi(J)$ はその零点全体の集合である．（代数幾何の言葉でいえば，A はイデアル J に対応する“0-次元代数多様体”である．）

以上のことをまとめて次の定理がえられる．

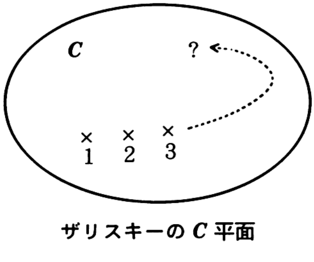
定理 5. $\mathscr{A}=\boldsymbol{C}$ の閉集合は $\phi,\boldsymbol{C}$，および任意の，定数でない $f(x)\in\boldsymbol{Q}[x]$ に対し，その零点全体からなる（代数的数の）有限集合である．

複素平面 $\boldsymbol{C}$ にこの“閉集合”の概念によって一つの位相を入れることができる．（この場合，A,B が閉集合ならば，$A\cup B$ も閉集合になる．証明してみて下さい．）この位相を（$\boldsymbol{Q}$ 上の）**ザリスキー**（Zariski）**位相**という．これはかなり変わった（しかし立派な）位相である．すぐわかるように，ハウスドルフ（Hausdorff）の分離公理は成り立たない．また，一点 $\{\alpha\}$ は $\alpha\in\boldsymbol{Q}$ のときに限って閉集合になる．α が超越数ならば，$\{\alpha\}$ の閉包は $\boldsymbol{C}$ 全体になる．二つの空でない開集合（閉集合の補集合）は必ず共通点をもつ！　しかも，$\boldsymbol{C}$ はこの位相に関してコンパクトである！

*　　*　　*

C君「コンパクトといっても，たとえば数列 1, 2, … は収束するのかしら？」

Bさん「それは任意の数に収束するのよ．一般に任意の無限列は任意の数に



ザリスキーの $\boldsymbol{C}$ 平面



収束する．ハウスドルフの分離公理が成立しないから，収束する点列の極限を特定することはできないのよ．」

A氏「やれやれ，少なくともわしはそんなややこしい位相空間に住みたいとは思わんね．」

＊　＊　＊

4.4. 共役系.　上のザリスキー閉集合をより精しく見るために，その既約分解を考える．

まず，定数でない多項式 $f(x) \in \boldsymbol{Q}[x]$ が（$\boldsymbol{Q}$ 上）**既約** であるとは，$f(x)$ の（$\boldsymbol{Q}[x]$ における）約数が“本質的に”（すなわち $\boldsymbol{Q}[x]$ の単数群 $\boldsymbol{Q}^\times$ の元による乗法を除いて）1 と $f(x)$ 自身しかないことをいう．たとえば，x^2-2 や x^2+1 は既約である．（すなわち，$\sqrt{2}$, $\sqrt{-1}$ は有理数でない！）しかし，$x^2-1=(x+1)(x-1)$ は既約でない（可約である）．x^2-1 は二つの既約多項式 $x+1$, $x-1$ の積である．

よく知られているように，$\boldsymbol{Q}[x]$ の任意の元 $f(x)$ は既約多項式の積として本質的に一意的に表される．（これは定理4からの帰結である．）いま，ザリスキー閉集合 $A \subset \boldsymbol{C}, A \neq \phi, \boldsymbol{C}$, の零化イデアルを $J=\varphi(A)$ とし，その最小多項式 $f_0(x)$ を既約因数に分解して

(8)
$$f_0(x) = \prod_{i=1}^{s} p_i(x)^{\nu_i}$$

とする．ただし，$p_i(x)$ は（相異なる）正規化された既約多項式，$\nu_i \in \boldsymbol{Z}$, $\nu_i > 0$ とする．（この分解は順序を除いて一意的に定まる．）ここで，実際はすべての $\nu_i=1$ である．すなわち

(8′)
$$f_0(x) = \prod_{i=1}^{s} p_i(x).$$

なぜならば，（8′）の右辺の多項式を $f_1(x)$ とおけば，$f_1(x) \in \boldsymbol{Q}[x]$ で，$f_1(x) \mid f_0(x)$ は明らかだが，$f_0(x)$ と $f_1(x)$ は同じ零点をもつから，$f_1(x) \in J$,

したがって $f_0(x) \mid f_1(x)$．よって $f_0(x)=f_1(x)$ である．

上の $f_0(x)$ のように相異なる既約多項式の積として表される多項式を **準既約** という．ここで準既約な多項式は重根をもたないことを注意しておこう．（したがって代数学の基本定理 * により，n 次の準既約多項式はちょうど n 個の相異なる根をもつ．）いま，(8′) の多項式 $f_0(x)$ が重根 α をもったとする．もし α が $p_i(x)$ の根ならば，それは $p_i(x)$ の重根であるか，またはある $p_j(x)$ ($j \neq i$) の根になる．これは $p_i(x)$ がその導関数 $p_i'(x)$，または $p_j(x)$ ($j \neq i$) と共通因子をもつこと，したがって（$p_i(x)$ は既約であるから）$p_i(x)$ 自身がこれらの多項式のいずれかの約数になることを意味する．しかし，これは明らかに矛盾である．

以上により

定理 6．$\boldsymbol{C}$ のザリスキー閉集合 $A \neq \phi, \boldsymbol{C}$ に対し，その零化イデアル $J=\varphi(A)$ の生成元（最小多項式）$f_0(x)$ は準既約である．(8′) をその既約分解とすれば，A は既約因子 $p_i(x)$ の零点の集合 P_i の直和（互いに共通部分のない和）になり，その元の個数は $\deg f_0(x)$ と一致する．逆に，任意の準既約多項式 $f_0(x)$ に対し，$J=(f_0(x))$ は $\boldsymbol{Q}[x]$ の閉集合である．

$\boldsymbol{Q}$ 上の既約多項式 $p(x)$ の零点の集合 $P=\{\alpha_1, \cdots, \alpha_n\}$ ($n=\deg p(x)$) を（$\boldsymbol{Q}$ 上の）**共役系** ということにする．これはいわば，（空でない）最小の閉集合である．一つの共役系に属する二つの α_i と α_j は（$\boldsymbol{Q}$上）互いに **共役** (conjugate) であるという．

いま α を任意の代数的数とし，$\{\alpha\}$ の閉包（すなわち $\{\alpha\}$ を含む最小の閉集合）を A とすれば，それは一つの共役系になる．したがって，α の最小多項式は既約である．また二つの代数的数が共役であるためには，その最小多項式が一致することが必要十分である．

共役系の例を少しあげてみよう．

$$\{1\},\quad \{-\frac{2}{3}\},\quad \{\sqrt{2}, -\sqrt{2}\},\quad \{2+\sqrt{3}, 2-\sqrt{3}\},$$

$$\{1+\sqrt{2+\sqrt{3}},\ 1+\sqrt{2-\sqrt{3}},\ 1-\sqrt{2+\sqrt{3}},\ 1-\sqrt{2-\sqrt{3}}\}.$$

これらに対応する（正規化された）既約多項式は

$$x-1,\ \ x+\frac{2}{3},\ \ x^2-2,\ \ (x-2)^2-3=x^2-4x+1,$$

$$((x-1)^2-2)^2-3=x^4-4x^3+2x^2+4x-2$$

である．代数的数 α はその最小多項式が n 次であるとき，n 次の無理数という．$\sqrt{2}$，$2+\sqrt{3}$ は2次，$1+\sqrt{2+\sqrt{3}}$ は4次の無理数である．

* * *

A氏の独白「いやはやどうも数学者は差別論者なのではないかね．それにただの有限集合が0次元代数多様体とは恐れ入った．わしの見るところ，数学者は同じことを新しい言葉で言い直すのがお好きな人種のようだね．」

* * *

4.5. ガロア理論. いよいよいわゆるガロア理論に入ることにしよう．

代数的数全体の集合を $\overline{\boldsymbol{Q}}$ で表す．そのとき，

定理7. $\overline{\boldsymbol{Q}}$ は $\boldsymbol{C}$ の部分体になる．

この定理の証明は次の節で与える．

$\overline{\boldsymbol{Q}}$ の自分自身の上への写像 σ が体の演算を保つとき，すなわち任意の $a, b\in\overline{\boldsymbol{Q}}$ に対し，

(A) $$(a+b)^\sigma=a^\sigma+b^\sigma,\qquad (ab)^\sigma=a^\sigma b^\sigma$$

が成立するとき，$\overline{\boldsymbol{Q}}$ の **自己同型** (automorphism) であるという．いままでの記法では $\sigma(a)$ とかくべきところであるが，便宜上 a^σ とかく．したがって，

$$a^{\sigma\tau}=(\sigma\tau)(a)=\sigma(\tau(a))=(a^\tau)^\sigma$$

である．自己同型 σ は加群の準同型であるから，前に述べたように，$0^\sigma=0$．また一つの体において $\{0,1\}$ は方程式 $x^2-x=0$ の解の集合として特徴づけられるから，集合として $\{0,1\}^\sigma=\{0^\sigma,1^\sigma\}=\{0,1\}$．よって $1^\sigma=1$ も成立する．$\overline{\boldsymbol{Q}}$ の自己同型全体の集合を $\mathrm{Aut}\,\overline{\boldsymbol{Q}}$ とかく．明らかに $\sigma,\tau\in\mathrm{Aut}\,\overline{\boldsymbol{Q}}$ のと

き，合成写像 $\sigma\cdot\tau$，逆写像 σ^{-1} もまた Aut $\overline{\boldsymbol{Q}}$ に属し，したがって Aut $\overline{\boldsymbol{Q}}$ はこの演算に関して群になる．これを $\overline{\boldsymbol{Q}}$ の自己同型群，または $\overline{\boldsymbol{Q}}/\boldsymbol{Q}$ の **ガロア (Galois) 群** という．

そこでわれわれは，次の設定を考える．

$\mathscr{A}$ = $\overline{\boldsymbol{Q}}$ =（代数的数全体の作る体），

$\mathscr{X}$ = Aut $\overline{\boldsymbol{Q}}$ =（体 $\overline{\boldsymbol{Q}}$ の自己同型群），

$\mathscr{R} = \{ (a, \sigma) \mid a^\sigma = a \}$.

このとき，$\mathscr{A} = \overline{\boldsymbol{Q}}$，$\mathscr{X}$ = Aut $\overline{\boldsymbol{Q}}$ の閉集合はどんなものになるか？

まず任意の $A \subset \overline{\boldsymbol{Q}}$ に対し，

$$\varphi(A) = \{ \sigma \in \mathrm{Aut}\, \overline{\boldsymbol{Q}} \mid a^\sigma = a \text{ for } \forall a \in A \}$$

は明らかに Aut $\overline{\boldsymbol{Q}}$ の部分群になる．これを A の（元別）**固定部分群** ということにしよう．（元別というのは A 全体の固定部分群 $\{ \sigma \in \mathrm{Aut}\, \overline{\boldsymbol{Q}} \mid A^\sigma = A \}$ と区別するためである．）一方，任意の $X \subset$ Aut $\overline{\boldsymbol{Q}}$ に対し，

$$\psi(X) = \{ a \in \overline{\boldsymbol{Q}} \mid a^\sigma = a \text{ for } \forall \sigma \in X \}$$

は $\overline{\boldsymbol{Q}}$ の部分体になる．実際，$a, b \in \psi(X)$ とすれば，すべての $\sigma \in X$ に対して，

$$(a+b)^\sigma = a^\sigma + b^\sigma = a + b,$$

$$(ab)^\sigma = a^\sigma \cdot b^\sigma = a \cdot b$$

が成立するから，$a+b, ab \in \psi(X)$，同様に $a-b \in \psi(X)$．すなわち，$\psi(X)$ は加減乗の演算に関して閉じている．上に述べたように，任意の自己同型 σ に対して，$0^\sigma = 0$，$1^\sigma = 1$ であるから，$0, 1 \in \psi(X)$．また $a \in \psi(X)$, $a \neq 0$ のとき

$$a^\sigma \cdot (a^{-1})^\sigma = (a \cdot a^{-1})^\sigma = 1^\sigma = 1.$$

よって

$$(a^{-1})^\sigma = (a^\sigma)^{-1} = a^{-1}.$$

すなわち $a^{-1} \in \psi(X)$．よって，$\psi(X)$ は 0 でない元による除法に関しても閉じている．結論として，$\psi(X)$ は（$\boldsymbol{C}$ におけると同じ演算で）体になる．よっ

て，それは $\overline{\boldsymbol{Q}}$ の部分体である．これを X の **固定部分体** という．（X の $\overline{\boldsymbol{Q}}$ における固定部分体を $\overline{\boldsymbol{Q}}^X$ とかくこともある．）

以上述べたことから，$\overline{\boldsymbol{Q}}$ の閉集合は部分体であり，Aut $\overline{\boldsymbol{Q}}$ の閉集合は部分群であることがわかった．逆に，$\overline{\boldsymbol{Q}}$ の任意の部分体，Aut $\overline{\boldsymbol{Q}}$ の任意の部分群は閉集合になるだろうか？ この疑問を解明するのが，これから説明しようとする $\overline{\boldsymbol{Q}}/\boldsymbol{Q}$ のガロア理論である．

4.6. 有限次代数体． また準備として，有限次代数体について少し説明しておく．一般に，$\boldsymbol{C}$ の部分体 F は $\boldsymbol{Q}$ 上のベクトル空間とみなすことができる．より一般に，F, F' を $\boldsymbol{C}$ の部分体，$F \subset F'$ とすれば，F' は F の上のベクトル空間になる．その次元を拡大 F'/F の **次数** といい，$[F':F]$ で表す．$[F':F]=n$ のとき，F' を F の n 次拡大体という．$\boldsymbol{Q}$ の有限次（n 次）拡大体を **有限次（n 次）代数体** という．（一般に $\overline{\boldsymbol{Q}}$ の部分体を **代数体** という．）

定理 8． $\alpha \in \boldsymbol{C}$ が代数的であるためには，ある有限次代数体 F があって $\alpha \in F$ となることが必要十分である．

（証明） n 次代数体 F があって，$\alpha \in F$ とする．そのとき $n+1$ 個の元

$$1,\ \alpha,\ \alpha^2,\ \cdots,\ \alpha^n$$

は $\boldsymbol{Q}$ 上一次従属であるから，すべては 0 でない $a_i \in \boldsymbol{Q}$ があって

$$\sum_{i=0}^{n} a_i \alpha^i = 0$$

となる．よって，$f(x) = \sum_{i=0}^{n} a_i x^i$ とおけば，$f(x) \in \boldsymbol{Q}[x]$, $f(x) \neq 0$, $f(\alpha) = 0$, したがって α は代数的である．逆に，α を代数的，$p(x)$ を α の最小多項式とすれば，（環の）準同型

$$f(x)\ (\in \boldsymbol{Q}[x]) \longmapsto f(\alpha)\ (\in \boldsymbol{C})$$

の核は $I(\alpha) = (p(x))$ である．いま，この準同型の像

$$\{ f(\alpha) \mid f(x) \in \boldsymbol{Q}[x] \}$$

を $\boldsymbol{Q}[\alpha]$ とかくことにすれば，環の準同型定理により自然な同型

$$\boldsymbol{Q}[x]/(p(x)) \cong \boldsymbol{Q}[\alpha] \tag{9}$$
$$(f(x) \bmod (p(x))) \longmapsto f(\alpha)$$

がえられる．（左辺の商環 $\boldsymbol{Q}[x]/(p(x))$ は体 $\boldsymbol{Q}$ を含むと考えてよい．そのとき，上の同型は $\boldsymbol{Q}$ の元をそれ自身にうつす．したがって，$\boldsymbol{Q}$ 上のベクトル空間の写像として $\boldsymbol{Q}$-線形である．）$p(x)$ は既約であるから，$(p(x))$ は極大イデアル，したがって $F=\boldsymbol{Q}[\alpha]$ は（α を含む）体になる．$n=\deg p(x)$ とすれば，(9) の左辺は明らかに

$$1,\ x,\ \cdots,\ x^{n-1} \quad (\bmod\ p(x))$$

を一つの底とする $\boldsymbol{Q}$ 上のベクトル空間である．よって，F は n 次代数体である．（証終）

定理 9.* F, F', F'' を $\boldsymbol{C}$ の部分体とする．

(i) F'/F, F''/F' が有限次拡大ならば，F''/F も有限次拡大で，$[F'':F]=[F'':F']\cdot[F':F]$.

(ii) F', F'' の"合成体"（F', F'' を含む $\boldsymbol{C}$ の部分体のうち最小なもの）を $K=F'\cdot F''$ とする．F'/F が有限次拡大ならば，K/F'' も有限次拡大で，$[K:F''] \leqq [F':F]$.

系. F'/F, F''/F が有限次拡大ならば，$F'\cdot F''/F$ も有限次拡大である．

定理 8 の証明に現れた体 $\boldsymbol{Q}[\alpha]$ は，$\boldsymbol{Q}$ 上"α によって生成される体"であるから，$\boldsymbol{Q}(\alpha)$ ともかく．また，$\boldsymbol{Q}$ 上二つの代数的数 α, β によって生成される体，すなわち合成体 $\boldsymbol{Q}(\alpha)\cdot\boldsymbol{Q}(\beta)$ を $\boldsymbol{Q}(\alpha,\beta)$ とかく．

定理 10.* F を有限次代数体とすれば，ある（代数的数）α があって $F=\boldsymbol{Q}(\alpha)$ とかける．

これらの定理の証明はたいていの抽象代数の教科書に出ているから，ここでは省略し，代わりにいくつかの数値例をあげておくことにする．

$$[\boldsymbol{Q}(\sqrt{2+\sqrt{3}}:\boldsymbol{Q}] = [\boldsymbol{Q}(\sqrt{2+\sqrt{3}}):\boldsymbol{Q}(\sqrt{3})]\cdot[\boldsymbol{Q}(\sqrt{3}):\boldsymbol{Q}]$$
$$= 2\cdot 2 = 4,$$
$$\boldsymbol{Q}(\sqrt{2}+\sqrt{3}) = \boldsymbol{Q}(\sqrt{2},\sqrt{3}) = \boldsymbol{Q}(\sqrt{2})\cdot\boldsymbol{Q}(\sqrt{3}),$$

$$[\boldsymbol{Q}(\sqrt{2}+\sqrt{3}):\boldsymbol{Q}]=4.$$

（読者はこれらの式を確かめてみて下さい.）

（定理7の証明）$\alpha, \beta \in \overline{\boldsymbol{Q}}$ とする．定理8により，ある有限次代数体 F, F' があって $\alpha \in F$, $\beta \in F'$．そのとき，明らかに $\alpha \pm \beta, \alpha\beta \in F \cdot F'$ であるが，定理9系により合成体 $F \cdot F'$ も有限次代数体である．また，$\alpha \neq 0$ ならば，$\alpha^{-1} \in F$．よって再び定理8により，$\alpha \pm \beta, \alpha\beta, \alpha^{-1} \in \overline{\boldsymbol{Q}}$．したがって，$\overline{\boldsymbol{Q}}$ は $\boldsymbol{C}$ の部分体である．　　　　　　　　　　　　　　　　　　（証終）

F を任意の代数体（$\overline{\boldsymbol{Q}}$ の部分体）とすれば，$\sigma \in \mathrm{Aut}\,\overline{\boldsymbol{Q}}$ に対し，

$$F^{\sigma} = \{\xi^{\sigma} \mid \xi \in F\}$$

も明らかに代数体になる．これを F の“共役体”という．すべての $\sigma \in \mathrm{Aut}\,\overline{\boldsymbol{Q}}$ に対して $F^{\sigma}=F$ である（すなわち F が $\mathrm{Aut}\,\overline{\boldsymbol{Q}}$ の作用に対して不変である）とき，F は（$\boldsymbol{Q}$ 上）**正規**（normal）であるという．$\boldsymbol{Q}[x]$ の元

$$f(x) = \prod_{i=1}^{n}(x-\alpha_i), \qquad \alpha_i \in \overline{\boldsymbol{Q}}$$

に対し，その根をすべて $\boldsymbol{Q}$ につけ加えてえられる体

$$F = \boldsymbol{Q}(\alpha_1, \cdots, \alpha_n)$$

は正規な有限次代数体である．（これを $f(x)$ の“最小分解体”という.）実際，任意の $\sigma \in \mathrm{Aut}\,\overline{\boldsymbol{Q}}$ に対して

$$\{\alpha_1^{\sigma}, \cdots, \alpha_n^{\sigma}\} = \{\alpha_1, \cdots, \alpha_n\}$$

であるから，

$$\boldsymbol{Q}(\alpha_1, \cdots, \alpha_n)^{\sigma} = \boldsymbol{Q}(\alpha_1^{\sigma}, \cdots, \alpha_n^{\sigma}) = \boldsymbol{Q}(\alpha_1, \cdots, \alpha_n),$$

すなわち $F^{\sigma}=F$ である．

定理11.　任意の有限次代数体に対し，それを含む正規な有限次代数体が存在する．

実際，任意の有限次代数体 F は，ある $\alpha \in \overline{\boldsymbol{Q}}$ によって $F=\boldsymbol{Q}(\alpha)$ とかける（定理10)．α の最小多項式を $p(x)$ とし，その最小分解体を F' とすれば，F' は F を含む正規な有限次代数体である．

便宜上，有限次代数体全部の集合を $\mathscr{F}$ とかくことにする．定理8, 9, 11 により，$\mathscr{F}$ は次の性質をもつ．

($\mathscr{F}$1)　$F, F' \in \mathscr{F} \implies F\cdot F' \in \mathscr{F}$.

($\mathscr{F}$2)　$\forall F \in \mathscr{F}$ に対し，ある正規な $F' \in \mathscr{F}$ があって $F \subset F'$.

($\mathscr{F}$3)　$\overline{\boldsymbol{Q}} = \bigcup_{F \in \mathscr{F}} F$.

4.7. 代数体は閉集合である.

表題の定理（次ページの定理14）を証明するためにもう少し準備をする．

F を代数体とし，F 上の多項式（すなわち F の元を係数とする多項式）の作る（可換）環を $F[x]$ で表す．これについても $\boldsymbol{Q}[x]$ について述べたことがそのまま成立する．すなわち，$F[x]$ のイデアルはすべて単項イデアルである，$F[x]$ の（0でも単数でもない）元は既約多項式の積に本質的に一意的に分解される，等々．また，任意の代数的数 α は F に対しても“代数的”である，すなわち $F[x]$ におけるある（0でない）既約多項式 $q(x)$ の零点になる．実際，α の $\boldsymbol{Q}$ における最小多項式を $p(x)$ とし，それを $F[x]$ において既約分解して

$$p(x) = \prod_{j=1}^{t} q_j(x)$$

とすれば，α はいずれか一つの $q_j(x)$ の零点になる．それを正規化したものが α の F における最小多項式である．

定理 12. F を代数体，$q(x)$ を $F[x]$ の既約多項式とし，α をその一つの零点とする．F 上 α によって生成される体を $F(\alpha)$ とすれば，次の自然な F-同型 σ_1 が存在する．

$$\sigma_1 : F[x]/(q(x)) \xrightarrow{\sim} F(\alpha),$$
$$\sigma_1(x \bmod (q(x))) = \alpha$$

（σ_1 が“F-同型”であるとは，σ_1 が体の同型であり，その F への制限 $\sigma_1|F$ が恒等写像になること，いいかえれば σ_1 が F-線形であることをいう．）

この証明は定理8の中で $\boldsymbol{Q}[x]$ について述べたことをそのまま $F[x]$ の場合に移せばよい．

定理13． F_1, F_2 を二つの代数体とし，（体の）同型 $\sigma_0 : F_1 \xrightarrow{\sim} F_2$ が与えられたとする．そのとき σ_0 は $\overline{\boldsymbol{Q}}$ の自己同型に拡張される．すなわち，ある $\sigma \in \mathrm{Aut}\,\overline{\boldsymbol{Q}}$ があって，$\sigma|F_1 = \sigma_0$ となる．

この定理の証明は「補遺2」で述べることにする．

定理14． A が $\mathscr{A} = \overline{\boldsymbol{Q}}$ の閉集合になるためには，A が $\overline{\boldsymbol{Q}}$ の部分体（すなわち代数体）になることが必要十分である．

（証明） A が閉集合ならば，代数体になることはすでに述べた．逆をいうために，F を任意の代数体とし，$\widetilde{F} = \psi(\varphi(F))$ とおく．$F = \widetilde{F}$ をいえばよい．$F \subset \widetilde{F}$ であることは一般論（定理2）から既知である．$F \supset \widetilde{F}$ でないとして矛盾を導こう．いま，ある代数的数 α があって，$\alpha \in \widetilde{F}, \notin F$ であるとする．α の F における最小多項式を $q(x)$ とし，

$$q(x) = \prod_{i=1}^{m} (x - \alpha_i), \qquad \alpha_i \in \overline{\boldsymbol{Q}}$$

とする．ここで $\alpha = \alpha_1$ としてよい．$\alpha \notin F$ であるから，$m > 1$ である．さて，定理12により，m 個の自然な F-同型

$$\sigma_i : F[x]/(q(x)) \xrightarrow{\sim} F(\alpha_i),$$
$$\sigma_i(x \bmod (q(x))) = \alpha_i$$

が存在する．$\sigma_0 = \sigma_2 \circ \sigma_1^{-1}$ とおけば，F-同型

$$\sigma_0 : F(\alpha) \xrightarrow{\sim} F(\alpha_2),$$
$$\sigma_0(\alpha) = \alpha_2$$

がえられる．定理13により σ_0 は $\overline{\boldsymbol{Q}}$ の自己同型に拡張される．すなわちある $\sigma \in \mathrm{Aut}\,\overline{\boldsymbol{Q}}$ があって，$\sigma|F(\alpha) = \sigma_0$ となる．σ_0 は F-同型であるから，$\sigma|F$ は恒等写像である．よって $\sigma \in \varphi(F)$．一方，$\alpha \in \widetilde{F} = \psi(\varphi(F))$ であるから，$\alpha^\sigma = \alpha$ でなければならない．これは

$$\alpha^\sigma = \sigma_0(\alpha) = \alpha_2 \neq \alpha$$

に矛盾する．（証終）

定理14の証明の中で述べたことにより，次の系がえられる．

系．二つの代数的数 α, β が（$\boldsymbol{Q}$ 上）共役であるためには，ある $\sigma \in \mathrm{Aut}\,\overline{\boldsymbol{Q}}$ があって，$\alpha^\sigma = \beta$ となることが必要十分である．

いいかえれば，（4.4で定義した）共役系は群 $\mathrm{Aut}\,\overline{\boldsymbol{Q}}$ の $\overline{\boldsymbol{Q}}$ における軌道（orbit）に他ならない．

4.8. クルルの位相.

次に，$\mathscr{X} = \mathrm{Aut}\,\overline{\boldsymbol{Q}}$ の閉集合がどんなものかを考える．それが $\mathrm{Aut}\,\overline{\boldsymbol{Q}}$ の部分群になることは既知（4.5）である．そこで，$G = \mathrm{Aut}\,\overline{\boldsymbol{Q}}$ とおき，H を G の任意の部分群とする．$\widetilde{H} = \varphi(\psi(H))$ は H を含む G の部分群であるが，これに関して次の定理が成立する．

定理15. $\sigma \in G$ とする．σ が $\widetilde{H}$ に属するためには，次の条件が成立することが必要十分である．

(K) 任意の有限次代数体 $F \in \mathscr{F}$ に対し，ある $\sigma' \in H$ があって，$\sigma|F = \sigma'|F$.

まず準備として，次の定理を証明する．

定理16 (Artin). K を $\boldsymbol{C}$ の部分体，G_1 を K の自己同型の作る有限群とし，

$$K_1 = \{\, \xi \in K \mid \xi^\sigma = \xi \text{ for } \forall \sigma \in G_1 \,\}$$

とおく．そのとき，K_1 は K の部分体，K/K_1 は有限次拡大で，

$$[K : K_1] = |G_1|. \tag{10}$$

（証明）K_1 が K の部分体になることは見やすい．（4.5に述べた通りである．）K_1 は G_1 の K における固定部分体 K^{G_1} である．

$\alpha \in K$ を任意にとり，その G_1 による像（orbit）

$$A = \{\, \alpha^\sigma \mid \sigma \in G_1 \,\}$$

を考える．A の元の個数を r とし，$A = \{\alpha_1, \cdots, \alpha_r\}$ とおく．$\alpha = \alpha_1$ としてよい．

$$f(x) = \prod_{i=1}^{r} (x - \alpha_i)$$

とおけば，$\sigma \in G_1$ の $K[x]$ への自然な作用に対して

$$f(x)^\sigma = \prod_{i=1}^{r}(x-\alpha_i{}^\sigma)$$

であるが，A は全体として σ-不変，すなわち集合として

$$\{\alpha_1^\sigma, \cdots, \alpha_r{}^\sigma\} = \{\alpha_1, \cdots, \alpha_r\}$$

であるから，$f(x)^\sigma = f(x)$．したがって，$f(x)$ の係数は K_1 に属する，すなわち $f(x) \in K_1[x]$．もし $f(x)$ が $K_1[x]$ において可約とすれば，A の真部分集合が G_1-不変ということになり矛盾である．よって，$f(x)$ は $K_1[x]$ において既約，したがって α の K_1 における最小多項式になる．よって

$$[K_1(\alpha):K_1] = \deg f(x) = r \leqq |G|.$$

$[K_1(\alpha):K_1]$ が最大になるような α をえらべば，$K_1(\alpha)=K$ となる．（もしそうでなければ，ある $\beta \in K, \notin K_1(\alpha)$ が存在する．そのとき $K_1(\alpha,\beta)/K_1$ は有限次拡大であるから定理10（の一般化）により，ある $\gamma \in K$ があって，$K_1(\alpha,\beta)=K_1(\gamma)$ となる．しかし，そのとき $[K_1(\gamma):K_1] > [K_1(\alpha):K_1]$ となり，これは α のとり方に矛盾する．）$K_1(\alpha)=K$ ならば，$\sigma \in G_1$ の K への作用は α^σ によって完全に定まる．よって，$|G|=r=[K:K_1]$ である．

（証終）

（定理15の証明） まず，条件（K）が必要であることを示す．F を任意の有限次代数体とする．定理11により，ある正規有限次代数体 K があって，$F \subset K$．いま，$\widetilde{H}$, H の元によって引き起こされる K の自己同型全体の作る（有限）群を G_1, G_1' とする．その固定部分体はそれぞれ

$$K^{G_1} = K \cap \psi(\widetilde{H}), \qquad K^{G_1'} = K \cap \psi(H)$$

であるが，$\psi(\widetilde{H}) = \psi(\varphi(\psi(H))) = \psi(H)$（定理1）であるから，それらは一致する．よってアルチンの定理（10）により

$$|G_1| = [K:K^{G_1}] = [K:K^{G_1'}] = |G_1'|.$$

明らかに $G_1 \supset G_1'$ であるから，$G_1 = G_1'$ である．このことは任意の $\sigma \in \widetilde{H}$ に対して，ある $\sigma' \in H$ があって，$\sigma|K = \sigma'|K$ となることを意味する．$F \subset K$

であるから，$\sigma|F=\sigma'|F$ も成立する．よって，任意の $\sigma\in\widetilde{H}$ に対して条件（K）が成り立つ．

逆に，$\sigma\in G$ に対して条件（K）が成立するとする．任意の $\alpha\in\psi(H)$ に対し，$F=\boldsymbol{Q}(\alpha)$ とおけば，F は有限次代数体である．よって条件（K）により，ある $\sigma'\in H$ があって，$\sigma|F=\sigma'|F$．しかし $\alpha\in\psi(H)$ であったから，$\alpha^{\sigma'}=\alpha$．よって $\alpha^{\sigma}=\alpha$．これがすべての $\alpha\in\psi(H)$ に対して成り立つから，$\sigma\in\varphi(\psi(H))=\widetilde{H}$ である． （証終）

条件（K）は，$\widetilde{H}=\varphi(\psi(H))$ があるトポロジーに関する H の閉包になっていることを示唆している．実際，次の節で示すように，G における“開集合”の概念を適当に定義すれば，それによって G は位相群になり，$\widetilde{H}$ はこの位相に関する H の閉包になることが証明される．これを**クルル**（Krull）**位相**という．したがって，$X\subset G=\mathrm{Aut}\,\overline{\boldsymbol{Q}}$ が以前の意味で“閉集合”になるためには，X がクルルの意味で閉部分群になることが必要十分なのである．

結論として，$\overline{\boldsymbol{Q}}/\boldsymbol{Q}$ のガロア理論を次のように述べることができる．

定理 17． 代数体 F, $\boldsymbol{Q}\subset F\subset\overline{\boldsymbol{Q}}$, の全体と $G=\mathrm{Aut}\,\overline{\boldsymbol{Q}}$ のクルル位相に関する閉部分群 H の全体の間には，（元別）固定部分群，固定部分体の関係：$H=\varphi(F)$, $F=\psi(H)$ による一対一対応が存在する．

4.9. 完全非連結な位相群.

まず，G における開集合の概念を次のように定義する．

（KT） $O\subset G$ は，任意の $\sigma\in O$ に対し，ある有限次代数体 $F\in\mathcal{F}$ があって，$\sigma\varphi(F)\subset O$ となるとき，G の開集合であるという．（空集合 ϕ は開集合であると考える．）

G の開集合全体の集合を $\mathcal{O}$ とかくことにする．

まず，$\sigma\varphi(F)$ 自身が開集合になることに注意しておく．実際，$\tau\in\sigma\varphi(F)$ ならば，ある $\rho\in\varphi(F)$ があって，$\tau=\sigma\rho$ とかける．$\varphi(F)$ が群であることから，$\rho\varphi(F)=\varphi(F)$，したがって $\tau\varphi(F)=\sigma\rho\varphi(F)=\sigma\varphi(F)$．よって，

$\sigma\varphi(F)$ は開集合の条件をみたしている．

次の定理が成立する．

定理 18. 上に定義した開集合の概念に関して G は位相空間になる．この位相はハウスドルフの分離公理を満足する．また，G はこの位相に関して位相群になる．

（証明）まず位相空間の条件をチェックする．

1. $O, O' \in \mathcal{O}$ ならば，$O \cap O' \in \mathcal{O}$.

実際，$\sigma \in O \cap O'$ とすれば，O, O' が開集合であることから，ある $F, F' \in \mathcal{F}$ があって，$\sigma\varphi(F) \subset O$, $\sigma\varphi(F') \subset O'$ となる．よって $F'' = F \cdot F'$ とすれば，$F'' \in \mathcal{F}$ で，$\sigma\varphi(F'') \subset \sigma\varphi(F) \cap \sigma\varphi(F') \subset O \cap O'$．よって $O \cap O'$ も開集合である．

2. I を（有限または無限の）添数の集合とし，$O_i \in \mathcal{O}$（$i \in I$）とする．そのとき $O = \bigcup_{i \in I} O_i \in \mathcal{O}$.

実際，$\sigma \in O$ とすれば，ある $i \in I$ に対して，$\sigma \in O_i$．よってある $F \in \mathcal{F}$ があって，$\sigma\varphi(F) \subset O_i \subset O$．よって O も開集合である．

3. ハウスドルフの分離公理がみたされる．

実際，$\sigma, \tau \in G$, $\sigma \neq \tau$ とすれば，ある $\alpha \in \overline{\boldsymbol{Q}}$ があって，$\alpha^\sigma \neq \alpha^\tau$．そのとき $F = \boldsymbol{Q}(\alpha)$ とおけば，$F \in \mathcal{F}$ で，$\sigma^{-1}\tau \notin \varphi(F)$．これから，$\varphi(F)$ が群であることにより，$\sigma\varphi(F) \cap \tau\varphi(F) = \phi$ がえられる．$O = \sigma\varphi(F)$, $O' = \tau\varphi(F)$ とおけば，上に注意したように，$O, O' \in \mathcal{O}$ で，明らかに $\sigma \in O$, $\tau \in O'$, $O \cap O' = \phi$ である．

次に，群の演算が連続であることをみる．

4. $\sigma, \tau \in G$, $O \in \mathcal{O}$, $\sigma\tau \in O$ とすれば，ある $O', O'' \in \mathcal{O}$ があって，$\sigma \in O'$, $\tau \in O''$, $O'O'' \subset O$.

5. $\sigma \in G$, $O \in \mathcal{O}$, $\sigma^{-1} \in O$ とすれば，ある $O' \in \mathcal{O}$ があって，$\sigma \in O'$, $O'^{-1} \subset O$.

（4の証明）仮定により，ある $F \in \mathcal{F}$ があって，$\sigma\tau\varphi(F) \subset O$．定理11に

より，正規な有限次代数体 F' で $F \subset F'$ となるものが存在する．そのとき，$O' = \sigma\varphi(F')$, $O'' = \tau\varphi(F')$ とおけば，$O', O'' \in \mathcal{O}$, $\sigma \in O'$, $\tau \in O''$ で，$\varphi(F')$ が G の正規部分群になることから，

$$O'O'' = \sigma\varphi(F') \cdot \tau\varphi(F') = \sigma\tau\varphi(F') \subset \sigma\tau\varphi(F) \subset O.$$

5の証明も全く同様であるから，読者に任せることにする． （証終）

この記号を使えば，定理15は

$$\widetilde{H} = \bigcap_{F \in \mathcal{F}} H \cdot \varphi(F) \tag{11}$$

とかくことができる．これはちょうどクルル位相に関する H の閉包に他ならない．

上に述べたように，$\sigma\varphi(F)$ （$F \in \mathcal{F}$）は開集合であるが，それは同時に閉集合でもある．実際，$\sigma\varphi(F)$ は部分群 $\varphi(F)$ による一つの傍系であるから，その補集合 $(\sigma\varphi(F))^c$ はこれと異なる傍系の和集合になる．したがって，それは開集合の和集合だから開集合になる．よって $\sigma\varphi(F)$ は閉集合である．

G のトポロジーの定義から，$\sigma \in G$ の基本近傍系として

$$\{\, \sigma\varphi(F) \mid F \in \mathcal{F} \,\}$$

をとることができる．上に述べたように，$\sigma\varphi(F)$ は開かつ閉な集合である．このことから，G の部分集合 $A \neq \phi$ が連結ならば，A は一点からなる集合であることがわかる．実際，もし $\sigma, \tau \in A$, $\sigma \neq \tau$ とすれば，ある $F \in \mathcal{F}$ があって，$\tau \notin \sigma\varphi(F)$．そこで $B = A \cap \sigma\varphi(F)$, $C = A \cap (\sigma\varphi(F))^c$ とおけば，B, C は A の空でない（相対的）開部分集合で，

$$A = B \cup C, \qquad B \cap C = \phi$$

となる．よって A は連結でない．

一般に，位相空間 $\mathscr{X}$ の連結部分集合が一点からなる集合のみであるとき，$\mathscr{X}$ は**完全非連結**であるという．したがって，次の定理がえられた．

定理19. $G = \mathrm{Aut}\,\overline{\boldsymbol{Q}}$ はクルル位相に関して完全非連結である．

*　　*　　*

Cさん「完全非連結な位相というのは，離散位相とはどう違うんですか？」

私「離散位相というのは一点が閉かつ開に，したがって任意の部分集合が閉かつ開になるような，本当に trivial な位相のことをいうのです．それに反して，完全非連結な位相というのはもっと実質のある位相です．補遺3で説明する p-進数体 $\boldsymbol{Q}_p$ の位相も完全非連結です．離散位相はもちろん完全非連結ですが，逆は有限集合の場合以外では成り立ちません．」

*　　*　　*

4.10. 中間拡大のガロア理論．　クルル位相が確立したところで，中間拡大に関するガロア理論をまとめておこう．

$G=\mathrm{Aut}\,\overline{\boldsymbol{Q}}$ とする．任意の代数体 F に対し，$\varphi(F)$ を改めて $\mathrm{Gal}(\overline{\boldsymbol{Q}}/F)$ とかくことにする．すなわち

$$\mathrm{Gal}(\overline{\boldsymbol{Q}}/F)=\{\sigma\in G\mid \alpha^\sigma=\alpha \text{ for } \forall\alpha\in F\}. \tag{12}$$

特に，$G=\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$．

K を $\overline{\boldsymbol{Q}}/F$ の中間体とする．任意の $\sigma\in\mathrm{Gal}(\overline{\boldsymbol{Q}}/F)$ に対し，K の共役 K^σ も $\overline{\boldsymbol{Q}}/F$ の中間体になる．すべての $\sigma\in\mathrm{Gal}(\overline{\boldsymbol{Q}}/F)$ に対し，$K^\sigma=K$ であるとき，拡大 K/F は**正規**であるという．正規拡大を**ガロア拡大**ともいう．（一般にガロア拡大とは分離的正規拡大のことをいうのであるが，この場合標数0であるから，“分離的”という条件は自動的にみたされている．）

さて，K/F を一つのガロア拡大とする．(12) を一般化して，K/F のガロア群を

$$\mathrm{Gal}(K/F)=\{\sigma\in\mathrm{Aut}\,K\mid \alpha^\sigma=\alpha \text{ for } \forall\alpha\in F\} \tag{13}$$

によって定義する．ただし，$\mathrm{Aut}\,K$ は体 K の自己同型全体の作る群である．任意の $\sigma\in\mathrm{Gal}(\overline{\boldsymbol{Q}}/F)$ は K を（全体として）不変にするから，K の自己同型を引き起こす．そのとき σ の K への制限 $\sigma|K$ は明らかに $\mathrm{Gal}(K/F)$ に属する．定理13によれば，逆に $\mathrm{Gal}(K/F)$ の任意の元はこのようにしてえられ

る．よって，自然な準同型

$$r_K\colon \mathrm{Gal}(\overline{\boldsymbol{Q}}/F) \longrightarrow \mathrm{Gal}(K/F)$$
$$\sigma \longmapsto \sigma|K$$

は“上へ”の写像になる．また，この準同型の核は明らかに $\mathrm{Gal}(\overline{\boldsymbol{Q}}/K)$ である．よって，準同型定理により自然な同型

$$\mathrm{Gal}(\overline{\boldsymbol{Q}}/F)/\mathrm{Gal}(\overline{\boldsymbol{Q}}/K) \cong \mathrm{Gal}(K/F) \tag{14}$$

がえられる．

さて，$\mathrm{Gal}(\overline{\boldsymbol{Q}}/F)$，$\mathrm{Gal}(\overline{\boldsymbol{Q}}/K)$ は $G=\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ の（クルル位相に関する）閉部分群であるから，それら自身も自然に位相群と考えられ，(14) の左辺は位相群としての商群になる．ガロア群 $\mathrm{Gal}(K/F)$ はこの意味で位相群と考えられる．そのとき，

$$\mathrm{Gal}(\overline{\boldsymbol{Q}}/K) \subset H \subset \mathrm{Gal}(\overline{\boldsymbol{Q}}/F) \tag{15}$$

となるような G の閉部分群 H は上の準同型で，閉部分群

$$\overline{H} \subset \mathrm{Gal}(K/F) \tag{15$'$}$$

と一対一に対応する．$\overline{\boldsymbol{Q}}/\boldsymbol{Q}$ のガロア理論（定理 17）により (15) の閉部分群 H には

$$K \supset E \supset F \tag{15$''$}$$

となるような代数体 E が，

$$E = \psi(H) = \overline{\boldsymbol{Q}}^H, \qquad H = \varphi(E) = \mathrm{Gal}(\overline{\boldsymbol{Q}}/E)$$

という関係で，一対一に対応する．そのとき，

$$E = K^{\overline{H}} = \{\alpha \in K \mid \alpha^\sigma = \alpha \text{ for } \forall\sigma \in \overline{H}\},$$
$$\overline{H} = \mathrm{Gal}(\overline{\boldsymbol{Q}}/E)/\mathrm{Gal}(\overline{\boldsymbol{Q}}/K) = \mathrm{Gal}(K/E)$$

である．

要約すれば，K/F がガロア拡大であるとき，(15$''$) における中間体 E と (15$'$) における閉部分群 $\overline{H}$ とは

$$\overline{H} = \mathrm{Gal}(K/E), \qquad E = K^{\overline{H}}$$

という関係で一対一に対応する．そのとき，（容易にわかるように）E が F の

上で正規になるためには，対応する $\overline{H}$ が Gal(K/F) の正規部分群になることが必要十分である．そしてこの条件がみたされているとき，自然な（位相群の）同型

$$\mathrm{Gal}(K/F)\,/\,\mathrm{Gal}(K/E) \cong \mathrm{Gal}(E/F) \tag{16}$$

が成立する．

特に K/F が有限次拡大であるとき，アルチンの定理により

$$|\,\mathrm{Gal}(K/F)\,| = [K:F] \tag{17}$$

が成立し，上述のことは通常の有限次拡大に関するガロア理論に帰着する．

ここでは中間拡大 K/F のガロア理論が $\overline{\boldsymbol{Q}}/\boldsymbol{Q}$ のガロア理論から導かれることを示したが，より抽象的に一般の（有限次または無限次の）ガロア拡大 K/F を定義し，そのガロア理論を（クルル位相の定義もこめて）直接 $\overline{\boldsymbol{Q}}/\boldsymbol{Q}$ の場合と同じように展開することもできる．興味のある読者は自分で検討してみられるとよいと思う．

第5章　ガロア理論のつづき
(円分体のガロア群)

この章は第4章のつづきである．ガロア群の位相を少し別の観点から眺め，それが有限群の“極限”とみなされることを説明する．また，ガロア群の重要な例として円分体の場合について述べる．（円分体のイデアル論については補遺4参照．）便宜上，節の番号を除き，式や定理の番号はすべて前章から継続するものとする．

5.1. 有限群の極限.　$\mathcal{F}$ を有限次代数体全部の集合とする．$\mathcal{F}' \subset \mathcal{F}$ は次の条件が成り立つとき，$\mathcal{F}$ において“等終”（cofinal）であるという．

(C)　すべての $F \in \mathcal{F}$ に対して，ある $F' \in \mathcal{F}'$ があって，$F \subset F'$.

たとえば，正規な有限次代数体全部の集合を $\mathcal{F}_0$ とすれば，$\mathcal{F}_0$ は $\mathcal{F}$ において等終である．

いま，$\mathcal{F}'$ を $\mathcal{F}$ の等終な部分集合とし，便宜上 $\mathcal{F}'$ の元に添数をつけて，

(18)
$$\mathcal{F}' = \{F_\lambda \ (\lambda \in \Lambda)\}$$

とかくことにする．そのとき，次の条件が成立する．

($\mathcal{F}'$1)　すべての $\lambda, \mu \in \Lambda$ に対して，ある $\nu \in \Lambda$ があって，$F_\lambda \cup F_\mu \subset F_\nu$.

($\mathcal{F}'$2)　すべての $\lambda \in \Lambda, \sigma \in G$ に対して，ある $\mu \in \Lambda$ があって，$F_\lambda^\sigma \subset F_\mu$.

($\mathcal{F}'$3)　$\bigcup_{\lambda \in \Lambda} F_\lambda = \overline{\boldsymbol{Q}}$.

（逆に $\mathcal{F}' \subset \mathcal{F}$ が（$\mathcal{F}'$3）をみたせば，$\mathcal{F}'$ は等終である．）

簡単のため，以下 $\mathcal{F}' \subset \mathcal{F}_0$ と仮定する．そのとき，条件（$\mathcal{F}'$2）は自然にみたされている．

$$N_\lambda = \mathrm{Gal}(\overline{\boldsymbol{Q}}/F_\lambda), \qquad \mathcal{N} = \{N_\lambda \ (\lambda \in \Lambda)\}$$

とおけば，N_λ は $G=\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ の正規部分群で，条件（$\mathscr{F}'1$），（$\mathscr{F}'3$）に対応して，次の条件が成立する．

(N1)　すべての $\lambda,\mu\in\Lambda$ に対して，ある $\nu\in\Lambda$ があって，$N_\nu\subset N_\lambda\cap N_\mu$，

(N3)　$\bigcap_{\lambda\in\Lambda} N_\lambda=\{1\}$.

（これらの条件は $\mathscr{N}$ が G における単位元 1 の一つの基本近傍系になるための条件と同じである．）

さて便宜上，Λ に次の仕方で“半順序”$\leq$ を定義する．

$$\lambda\leq\mu \iff N_\lambda\supset N_\mu\ (\iff F_\lambda\subset F_\mu).$$

そのとき，(N1) あるいは（$\mathscr{F}'1$）により

(Λ)　すべての $\lambda,\mu\in\Lambda$ に対し，ある $\nu\in\Lambda$ があって，$\lambda\leq\nu,\ \mu\leq\nu$.

この条件をみたす半順序集合を“有向集合”という．

さて，

$$G_\lambda = G/N_\lambda = \mathrm{Gal}(F_\lambda/\boldsymbol{Q}) \tag{19}$$

とおけば，$\lambda\leq\mu$ のとき，自然な準同型

$$\varphi_{\lambda\mu}: G_\mu \longrightarrow G_\lambda \tag{20}$$

が存在する．（$\sigma\in G_\mu$ に対し，$\varphi_{\lambda\mu}(\sigma)=\sigma|F_\lambda$ と定義する．）この準同型に対し，明らかに

$$\lambda\leq\mu\leq\nu \implies \varphi_{\lambda\mu}\circ\varphi_{\mu\nu} = \varphi_{\lambda\nu} \tag{21}$$

が成立する．

いま，$\sigma\in G$ に対して，$\sigma_\lambda=\sigma|F_\lambda$ とおけば，明らかに

$$\lambda\leq\mu \implies \sigma_\lambda = \varphi_{\lambda\mu}(\sigma_\mu) \tag{22}$$

が成立する．逆に，すべての $\lambda\in\Lambda$ に対して $\sigma_\lambda\in G_\lambda$ が与えられ，(22) が成り立つとすれば，$\sigma|F_\lambda=\sigma_\lambda$ となるような G の元 σ がただ一つ定まる．（（$\mathscr{F}'3$）により，任意の $\alpha\in\overline{\boldsymbol{Q}}$ に対し，ある $\lambda\in\Lambda$ があって，$\alpha\in F_\lambda$．よって，$\alpha^\sigma=\alpha^{\sigma_\lambda}$ とおけばよい．（$\mathscr{F}'1$），(22) により，σ は矛盾なく定義され，$\overline{\boldsymbol{Q}}$ の一つの自己同型になる．）よって，

(23) $$\widetilde{G} = \{ (\sigma_\lambda)_{\lambda \in \Lambda} \mid \sigma_\lambda \in G_\lambda,\ \text{satisfying (22)} \}$$

とおけば，自然な同型 $G \cong \widetilde{G}$ が成立する．($\widetilde{G}$ における積は $(\sigma_\lambda)\cdot(\tau_\lambda) = (\sigma_\lambda \tau_\lambda)$ によって定義する．)

一般に，Λ を一つの有向集合とし，群の集合 $\{ G_\lambda\ (\lambda \in \Lambda) \}$，およびそれらの間の準同型の集合

$$\{ \varphi_{\lambda\mu}\ (\lambda, \mu \in \Lambda,\ \lambda \leq \mu) \}$$

が与えられ，$\varphi_{\lambda\lambda} = 1$（$G_\lambda$ の恒等写像）で，条件 (21) が成立するとき，(23) によって新しい群 $\widetilde{G}$ を定義することができる．この群を $\{ G_\lambda, \varphi_{\lambda\mu}\ (\lambda, \mu \in \Lambda) \}$ の**射影極限**といい，

$$\widetilde{G} = \varprojlim_{\lambda} G_\lambda$$

とかく．

さらに G_λ が位相群で，$\varphi_{\lambda\mu}$ が連続な準同型ならば，$\widetilde{G}$ に自然な位相が定義される．すなわち，まず直積

$$\dot{G} = \prod_{\lambda \in \Lambda} G_\lambda$$

は直積空間の位相（弱位相）に関して位相群になり，$\widetilde{G}$ はその閉部分群になる．したがって，$\widetilde{G}$ も位相群になる．

($\dot{G}$ の単位元の基本近傍系 $\mathcal{U}$ は次のように定義される．$\{ \lambda_1, \cdots, \lambda_k \}$ を Λ の任意の有限部分集合，各 λ_i に対し U_{λ_i} を G_{λ_i} の単位元の一つの基本近傍系に属する任意の近傍とするとき，$\mathcal{U}$ は

$$U = \{ (\sigma_\lambda) \mid (\sigma_\lambda) \in \dot{G},\ \sigma_{\lambda_i} \in U_{\lambda_i}\ (1 \leqq i \leqq k) \}$$

の形の部分集合全体の集合．)

われわれが考えているガロア群の場合には，G_λ は有限群であるから，自然な離散位相に関してコンパクトである．したがって（チコノフ (Tychonoff) の定理により）直積 $\dot{G}$ もコンパクトであり，その閉部分群 $\widetilde{G}$ もコンパクトである．自然な同型 $\varphi : G \cong \widetilde{G}$ において，$\varphi(\sigma) = (\sigma_\lambda)$ とすれば，$\sigma_\lambda = \sigma | F_\lambda$ であるから

$$\sigma \in N_\lambda \iff \sigma_\lambda = 1.$$

これは G のクルル位相がちょうど $\widetilde{G}$ の上記の位相を移したものになっていることを示す．したがって，位相群としての同型

(24) $$G \cong \varprojlim_{\lambda} G_\lambda$$

が成立する．特にガロア群 G はコンパクトであることがわかった．

以上をまとめて，次の定理がえられた．

定理20． $\{F_\lambda\ (\lambda \in \Lambda)\}$ を正規な有限次代数体からなる（有向）集合で $(\mathcal{F}'1)$, $(\mathcal{F}'3)$ をみたすものとし，$G_\lambda = \mathrm{Gal}(F_\lambda/\boldsymbol{Q})$ とおけば，自然な準同型 $\varphi_{\lambda\mu}: G_\mu \to G_\lambda$ に関して，射影極限 $\varprojlim_{\lambda} G_\lambda$ が定義される．そのとき，$G = \mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ は（クルル位相により，位相群として）$\varprojlim_{\lambda} G_\lambda$ と同一視される．特に G はコンパクトである．

4.10 で説明したように，中間拡大のガロア群 $\mathrm{Gal}(K/F)$ についても全く同様な結果がえられる．

5.2．円分体のガロア群． 最後に無限次ガロア拡大の典型的な例として，円分体を考えてみよう．

準備として，商環 $\boldsymbol{Z}/n\boldsymbol{Z}$ の考察から始める．第2章において，加群として商群 $\boldsymbol{Z}/n\boldsymbol{Z}$ を考えたが，$\boldsymbol{Z}$ は 1 をもつ可換環で，$n\boldsymbol{Z}$ はそのイデアルであるから，環としての商 $\boldsymbol{Z}/n\boldsymbol{Z}$ が定義される．$a \in \boldsymbol{Z}$ の $\mathrm{mod}\, n\boldsymbol{Z}$ の剰余類を $[a] = a + n\boldsymbol{Z}$ とかくことにすれば，積は

$$[a]\cdot[b] = [ab]$$

によって定義される．$n\boldsymbol{Z}$ がイデアルだから，このようにして積が矛盾なく定義されるのである．（以下，$\mathrm{mod}\, n$ と $\mathrm{mod}\, n\boldsymbol{Z}$ とを混用するが，意味は全く同じである．）

1 をもつ可換環 $\boldsymbol{Z}/n\boldsymbol{Z}$ において，$[a]$ が可逆であるためには，次の互いに同値な条件が成立することが必要十分である．

1） $ax \equiv 1 \pmod{n}$ となるような $x \in \boldsymbol{Z}$ が存在する．

2） $ax+ny=1$ をみたす $x, y \in \boldsymbol{Z}$ が存在する．

3） $(a, n)=1$ すなわち a と n は互いに素である．

（これらの条件が同値であることは初等整数論でよく知られている．）これらの条件がみたされるとき，$[a]$を“既約剰余類”という．すなわち，商環 $\boldsymbol{Z}/n\boldsymbol{Z}$ の単数群 $(\boldsymbol{Z}/n\boldsymbol{Z})^{\times}$ は既約剰余類の作る乗法群である．これらの剰余類の $\bmod n$ の代表系として

$$\{ k \in \boldsymbol{Z} \mid 1 \leqq k \leqq n-1,\ (k, n)=1 \}$$

をとることができる．簡単のため，この集合を $R_n^{\times}$ とかくことにする．また $R_n^{\times}$ の元の個数 $|(\boldsymbol{Z}/n\boldsymbol{Z})^{\times}|$ を $\varphi(n)$ で表す．$\varphi(n)$ は“オイラー関数”と呼ばれている．

特に n が素数 p のときには

$$1 \leqq k \leqq p-1 \implies (k, p)=1$$

であるから，

$$(\boldsymbol{Z}/p\boldsymbol{Z})^{\times} = (\boldsymbol{Z}/p\boldsymbol{Z}) - \{0\}, \qquad \varphi(p) = p-1$$

である．したがって，$\boldsymbol{Z}/p\boldsymbol{Z}$ は体になる．

自然数 n に対して，$\zeta_n = e^{2\pi i/n}$ とおけば，1の n 乗根（すなわち，$x^n-1=0$ の根）の全体は

(25)
$$\mu_n = \{ 1, \zeta_n, \zeta_n^2, \cdots, \zeta_n^{n-1} \}$$

で与えられる．μ_n は位数 n の巡回群になる．容易にわかるように，ζ_n^k がこの群の生成元になるためには，$(k, n)=1$ であること，すなわち $[k]$ が既約剰余類になることが必要十分である．このとき，ζ_n^k を“1の原始 n 乗根”という．

さて，$\sigma \in G = \mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ とすれば，$x^n-1 \in \boldsymbol{Q}[x]$ であるから，その根の集合 μ_n は全体として σ-不変である．特に ζ_n^{σ} は μ_n の生成元になるから，

(26)
$$\zeta_n^{\sigma} = \zeta_n^{k(\sigma)}, \qquad k(\sigma) \in R_n^{\times}$$

とかくことができる．そのとき，次の定理が成立する．

定理21． 写像

$$\sigma\ (\in G)\ \longmapsto\ k(\sigma)\ (\bmod n\boldsymbol{Z}) \tag{27}$$

は $G=\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ から $(\boldsymbol{Z}/n\boldsymbol{Z})^{\times}$ の上への準同型を与える．

（証明）この写像が準同型であることは次のようにしてわかる．$\sigma,\tau\in G$ とすれば，

$$\zeta_n^{\sigma\tau} = (\zeta_n^{\tau})^{\sigma} = (\zeta_n^{k(\tau)})^{\sigma} = (\zeta_n^{\sigma})^{k(\tau)} = \zeta_n^{k(\sigma)\,k(\tau)}.$$

よって $k(\sigma\tau)\equiv k(\sigma)k(\tau)\ (\bmod n)$．よって写像（27）は準同型である．

この写像が“上へ”の準同型になることは，ζ_n の共役系が 1 の原始 n 乗根の全体 $\{\zeta_n^k \mid k\in R_n^{\times}\}$ と一致すること，いいかえれば“円分多項式”

$$\Phi_n(x) = \prod_{k\in R_n^{\times}}(x-\zeta_n^k) \tag{28}$$

が $\boldsymbol{Q}[x]$ の既約多項式になることと同値である．$\Phi_n(x)$ はすべての $\sigma\in G$ に対して不変であるから，$\boldsymbol{Q}[x]$ に属することは明らかである．それが既約であることの証明はたいていの抽象代数（または整数論）の教科書に載っているからここでは省略する.*（補遺4にも一つの証明を与える．）　（証終）

上の定理によれば，$\Phi_n(x)$ は $\varphi(n)$ 次の（正規化された）既約多項式である．明らかに

$$x^n-1 = \prod_{d\mid n}\Phi_d(x)$$

という関係が成立する．したがって，$\Phi_1(x)=x-1$ から出発して，$\Phi_n(x)$ を帰納的に求めることができる．（このことから，実際 $\Phi_n(x)\in\boldsymbol{Z}[x]$ であることがわかる．）たとえば，

$$x^2-1 = \Phi_1(x)\Phi_2(x),$$
$$x^5-1 = \Phi_1(x)\Phi_5(x),$$
$$x^{10}-1 = \Phi_1(x)\Phi_2(x)\Phi_5(x)\Phi_{10}(x)$$

であるから，

$$\Phi_2(x) = x+1,\qquad \varphi(2)=1,$$
$$\Phi_5(x) = x^4+x^3+x^2+x+1,\qquad \varphi(5)=4,$$

$$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1, \quad \varphi(10) = 4.$$

“円分体” $\boldsymbol{Q}(\zeta_n)$ は x^n-1（または $\Phi_n(x)$）の最小分解体であるから，正規である．定理21において準同型（27）の核は明らかに $\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q}(\zeta_n))$ であるから，準同型定理と（14）により，自然な同型

(29) $$\mathrm{Gal}(\boldsymbol{Q}(\zeta_n)/\boldsymbol{Q}) \cong (\boldsymbol{Z}/n\boldsymbol{Z})^\times$$

がえられる．

ここで，この定理の2次体論への一つの応用を与えておこう．3.8 で定義したガウスの和

$$\gamma = \sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\zeta_p^k$$

を考える．$\boldsymbol{Q}(\gamma) \subset \boldsymbol{Q}(\zeta_p)$ であるが，$\gamma^2 = \left(\frac{-1}{p}\right)p$ であるから，$\boldsymbol{Q}(\gamma)$ は2次の代数体になる．（これを単に“2次体”という．実際，$\boldsymbol{Q}(\gamma)$ は $\boldsymbol{Q}(\zeta_p)$ に含まれる唯一の2次体である．）

さて，$\sigma \in \mathrm{Gal}(\boldsymbol{Q}(\zeta_p)/\boldsymbol{Q})$ に対して（26）によって $k(\sigma)$ を定義すれば，

$$\begin{aligned}\gamma^\sigma &= \sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\zeta_p^{k(\sigma)k} \\ &= \left(\frac{k(\sigma)}{p}\right)\gamma\end{aligned}$$

であるから，

(30) $$\gamma^\sigma = \gamma \iff \left(\frac{k(\sigma)}{p}\right) = 1.$$

がえられる．いいかえれば，

定理22. $\gamma = \sqrt{\varepsilon p}$, $\varepsilon = \left(\frac{-1}{p}\right)$ とすれば，

$$\mathrm{Gal}(\boldsymbol{Q}(\zeta_p)/\boldsymbol{Q}(\gamma)) = \left\{\sigma \in \mathrm{Gal}(\boldsymbol{Q}(\zeta_p)/\boldsymbol{Q}) \;\middle|\; \left(\frac{k(\sigma)}{p}\right) = 1\right\}.$$

次の章で説明するように，この定理から $\boldsymbol{Q}(\gamma)$ における素イデアルの分解法則，平方剰余の相互法則などが容易に導かれる．2次体の整数論もそれを円分体の中に埋め込んで考えるとき，はじめてその意味が明瞭になるのである．

5.3. 極限への移行.　さて自然数の集合 $\boldsymbol{N}$ に通常の大小関係ではなく，乗除関係で半順序を定義する．すなわち $n|m$ のとき，m の方が“大きい”と考えるのである．よく知られているように，$n\in\boldsymbol{N}$ は素数ベキの積として

$$n = \prod_{i=1}^{r} p_i^{\nu_i}$$

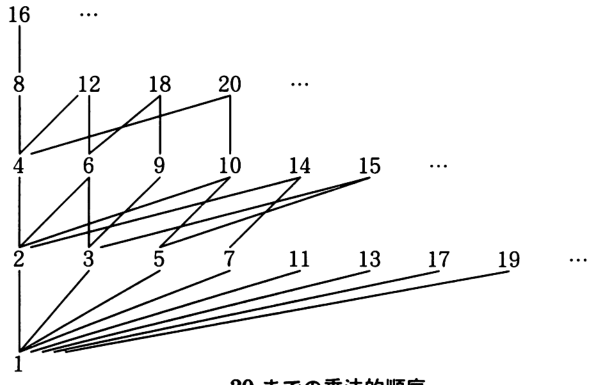
の形に（順序を除いて）一意的に表される．任意の素数 p に対して

$$\nu_p(n) = \begin{cases} \nu_i & p = p_i \text{ のとき} \\ 0 & \text{そうでないとき} \end{cases}$$

とおく．この記号を使えば，

(31)
$$n|m \iff \nu_p(n) \le \nu_p(m) \text{ for } \forall p$$

である．明らかに，$\boldsymbol{N}$ はこの半順序に関して有向集合になる．



20 までの乗法的順序

さて，$n, m\in\boldsymbol{N}$, $n|m$ であるとき，$n\boldsymbol{Z}\supset m\boldsymbol{Z}$ であるから，自然な環の準同型

(32)
$$\psi_{nm} : \boldsymbol{Z}/m\boldsymbol{Z} \longrightarrow \boldsymbol{Z}/n\boldsymbol{Z}$$
$$(a \bmod m\boldsymbol{Z}) \longmapsto (a \bmod n\boldsymbol{Z})$$

が定義される．これは自然に群の準同型

$$\psi_{nm}^{\times} : (\boldsymbol{Z}/m\boldsymbol{Z})^{\times} \longrightarrow (\boldsymbol{Z}/n\boldsymbol{Z})^{\times}$$

を引き起こす．一方，$\boldsymbol{Q}(\zeta_n) \subset \boldsymbol{Q}(\zeta_m)$ となるから，自然な準同型

$$(33) \qquad \begin{aligned} \varphi_{nm} : \mathrm{Gal}\,(\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q}) &\longrightarrow \mathrm{Gal}\,(\boldsymbol{Q}(\zeta_n)/\boldsymbol{Q}) \\ \sigma &\longmapsto \sigma|\boldsymbol{Q}(\zeta_n) \end{aligned}$$

が存在する．そして，これらの準同型に関して（定義式（26）から容易にわかるように）次の図式は可換になる．

$$\begin{array}{ccc} \mathrm{Gal}\,(\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q}) & \longrightarrow & (\boldsymbol{Z}/m\boldsymbol{Z})^\times \\ \varphi_{nm} \downarrow & & \downarrow \psi_{nm}^\times \\ \mathrm{Gal}\,(\boldsymbol{Q}(\zeta_n)/\boldsymbol{Q}) & \longrightarrow & (\boldsymbol{Z}/n\boldsymbol{Z})^\times \end{array}$$

よって，$\boldsymbol{N}$ の（乗法的）半順序に関する射影極限をとることにより，同型

$$(34) \qquad \varprojlim_n \mathrm{Gal}\,(\boldsymbol{Q}(\zeta_n)/\boldsymbol{Q}) \cong \varprojlim_n (\boldsymbol{Z}/n\boldsymbol{Z})^\times$$

がえられる．

そこで $K = \bigcup_{n=1}^{\infty} \boldsymbol{Q}(\zeta_n)$ とおけば，5.1 で述べたことから，（34）の左辺は（位相群として）$\mathrm{Gal}\,(K/\boldsymbol{Q})$ と同一視される．一方，

$$\boldsymbol{Z}/n\boldsymbol{Z} \cong \prod_p (\boldsymbol{Z}/p^{\nu_p(n)}\boldsymbol{Z})$$

であり，「補遺 3」で説明するように，$\boldsymbol{N}$ の通常の順序に関して

$$\varprojlim_\nu (\boldsymbol{Z}/p^\nu\boldsymbol{Z}) = \boldsymbol{Z}_p$$

は（位相環として）“p-進整数” の環と一致する．よって（34）の右辺は

$$\begin{aligned} \varprojlim_n (\boldsymbol{Z}/n\boldsymbol{Z})^\times &= \prod_p \varprojlim_\nu (\boldsymbol{Z}/p^\nu\boldsymbol{Z})^\times \\ &= \prod_p \boldsymbol{Z}_p^\times \end{aligned}$$

となる．

結論として，

定理 23. $K = \bigcup_{n=1}^{\infty} \boldsymbol{Q}(\zeta_n)$ とすれば，位相群としての自然な同型

$$(35) \qquad \mathrm{Gal}\,(K/\boldsymbol{Q}) \cong \prod_p \boldsymbol{Z}_p^\times$$

が成立する．

この定理に関連して二つのこと（実は一つのこと）を述べておく必要がある．第一に，円分体 $\boldsymbol{Q}(\zeta_n)$ のガロア群 $\mathrm{Gal}(\boldsymbol{Q}(\zeta_n)/\boldsymbol{Q})$ はアーベル群であるから，拡大 $\boldsymbol{Q}(\zeta_n)/\boldsymbol{Q}$ は“アーベル拡大”であり，それらの合成である $K/\boldsymbol{Q}$ は（無限次）アーベル拡大である．しかし，実際 K は $\boldsymbol{Q}$ の<u>最大</u>アーベル拡大体になる．すなわち，$\boldsymbol{Q}$ の任意のアーベル拡大はある円分体に含まれる．（2次体が円分体に含まれることはすでに見た通りである．）これが有名な**クロネッカー**（Kronecker）**の定理**（1853）である．（完全な証明は後に Weber によって与えられた．）G の交換子群 $[G, G]$ の閉包による商群を G^{ab} とかけば，この定理は $G^{ab} = \mathrm{Gal}(K/\boldsymbol{Q})$ であることを意味する．

第二に，(35) の右辺に現れる群は $\boldsymbol{Q}$ のいわゆる“イデール群”の有限部分の開部分群である．一般に“類体論”* によって，有限次代数体のアーベル拡大 K/F のガロア群はその基礎体 F のイデール類群で（非分岐な場合はイデアル類群で）記述され，それによって拡大 K/F における素イデアルの分解の状態を精しく知ることができる．上の定理 21, 23 はこの類体論の対応の“原型”を与えるものである．円分体における素イデアルの分解法則については「補遺4」で（その部分体である2次体の場合については次の章で）簡単に説明することにしよう．この本ではこれ以上説明できないが，類体論ばかりでなく，整数論における重要な理論，岩沢理論や虚数乗法論など，その根源はみな円分体の理論にあるといっても過言ではなかろう．

5.4. 類体論とは？　＊　＊　＊

C君 「その類体論って一体どんな理論ですか？」

私 「まず有限次代数体 F に対して“イデアル類群”というものがある．これは F の整数環 $\mathcal{O}_F$ の分数イデアルの作る群を単項イデアルの群で割ってできる商群のことだ (6.5, 例3, A4.2, 定理7参照)．それは有限アーベル群になる．ヒルベルトは前世紀末頃，虚2次体上の虚数乗法論の結果などから類推して，任意の F に対してその非分岐なガロア拡大で，そのガロア

群が F のイデアル類群と同型になるものが存在するだろうという予想をたてた．これが“絶対類体”と呼ばれるものだ．」

C君 「不思議な体ですね．」

私 「この類体の存在，一意性，etc. はフルトウェングラー（Furtwängler）によって証明された．この絶対類体では F のイデアルはすべて単項イデアルになる，など面白い性質がある．この意味で絶対類体は非常に特別な体なのだ．たとえば，$\boldsymbol{Q}$ の絶対類体は一体何になるか？」

C君 「$\boldsymbol{Q}$ の整数環 $\boldsymbol{Z}$ は単項イデアル環だから，そのイデアル類群は単位元だけしかない群になる．そうすると絶対類体は $\boldsymbol{Q}$ 自身になってしまう？」

私 「その通り．実際，$\boldsymbol{Q}$ の非分岐な拡大体は（アーベル拡大と限らなくても）trivial なもの，すなわち $\boldsymbol{Q}$ 自身しかないことが知られている．ところが高木貞治は1910年代に，ウェーバー（Weber）の拡張された意味のイデアル類群を使えば，事情は一変して F のすべての有限次アーベル拡大は類体としてえられるということを発見した．つまり

「相対アーベル体」＝「類体」

ということだ．前に言ったクロネッカーの定理はこの“等式”の $F=\boldsymbol{Q}$ の場合に他ならない．」

C君 「そのへんをもうちょっと説明して下さい．」

私 「まず同型（29）の右辺をみると，$(\boldsymbol{Z}/n\boldsymbol{Z})^{\times}$ という群がでてくる．これが，実は $\boldsymbol{Q}$ の場合のウェーバーのイデアル類群になるのだ．少しややこしいが，その説明から始めることにしよう．いま 0 でない有理数 $a=b/c$ で“n と無縁な”もの（すなわち，分母分子 b, c がともに n と素になるもの）全体を $\boldsymbol{Q}^{(n)}$，その中で特に $a>0$ であるもの全体を $\boldsymbol{Q}^{(np_\infty)}$ とかくことにする（それらはいずれも乗法群になる）．$\boldsymbol{Q}^{(n)}$ の元から生じる（単項）イデアルの群を $\mathscr{T}^{(n)}$ とすれば，

$$\mathscr{T}^{(n)}=\boldsymbol{Q}^{(n)}/\{\pm 1\}\cong\boldsymbol{Q}^{(np_\infty)}$$

となる．さらに分母分子 b, c が

$$(b, n) = 1, \quad b \equiv c \pmod{n}, \quad bc > 0$$

という条件をみたす有理数全体（それも群になる）を $\boldsymbol{Q}^\times(n\mathfrak{p}_\infty)$，この群の元から生じる単項イデアルの群を $\mathcal{P}(n\mathfrak{p}_\infty)$ とすれば，

$$\mathcal{P}(n\mathfrak{p}_\infty) = (\boldsymbol{Q}^\times(n\mathfrak{p}_\infty)\cdot\{\pm1\})/\{\pm1\} \cong \boldsymbol{Q}^\times(n\mathfrak{p}_\infty).$$

したがって

$$(36) \qquad \mathcal{I}^{(n)}/\mathcal{P}(n\mathfrak{p}_\infty) \cong \boldsymbol{Q}^{(n\mathfrak{p}_\infty)}/\boldsymbol{Q}^\times(n\mathfrak{p}_\infty)$$

となる．この左辺の群がこの場合の（n を法とする）拡張されたイデアル類群（ray class group）なのだ．一方，この右辺の商群の代表元としてはいつでも

$$a \in \boldsymbol{Z}, \quad (a, n) = 1, \quad a > 0,$$

をみたすものをとることができ，この条件をみたす二つの元 a, a' に対して，

$$a \equiv a' \pmod{n} \iff \frac{a}{a'} \in \boldsymbol{Q}^\times(n\mathfrak{p}_\infty)$$

が成り立つ（つまり加法的合同と乗法的合同とが同値になる）．したがって，(36) から

$$(36') \qquad \mathcal{I}^{(n)}/\mathcal{P}(n\mathfrak{p}_\infty) \cong (\boldsymbol{Z}/n\boldsymbol{Z})^\times.$$

これで群 $(\boldsymbol{Z}/n\boldsymbol{Z})^\times$ が拡張されたイデアル類群と同一視されることがわかった．よって (29) をかき直して

$$(29') \qquad \mathrm{Gal}(\boldsymbol{Q}(\zeta_n)/\boldsymbol{Q}) \cong \mathcal{I}^{(n)}/\mathcal{P}(n\mathfrak{p}_\infty)$$

という同型がえられる．この式は円分体 $\boldsymbol{Q}(\zeta_n)$ がちょうど拡張されたイデアル類群 $\mathcal{I}^{(n)}/\mathcal{P}(n\mathfrak{p}_\infty)$ に対応する高木の意味の類体になっていることを示すものなのだ．類体論の基本定理によって $\boldsymbol{Q}$ の任意のアーベル拡大はこの意味の類体（いまの場合は円分体）に含まれるから，クロネッカーの定理がでてくる．（もちろん，クロネッカーの定理は類体論以前に証明されていたのだが.）一般の F の場合にも，同じようにして拡張されたイデアル類群が定義される．そして F の任意のアーベル拡大は“類体”に

なる，すなわちあるイデアル類群に対応し，そのガロア群とイデアル類群とが同型になっているのだ.」

C君「なるほど，そうすると $\boldsymbol{Q}$ の場合，アーベル体は類体なり，類体は円分体なり，よってアーベル体は円分体なり，というわけなのですね．ところで，アルチンの相互律というのは何ですか？」

私「それはいま言ったガロア群とイデアル類群の同型が単に同型というだけではなく，素イデアルの分解法則などを含んでいるということだ．円分拡大 $\boldsymbol{Q}(\zeta_n)/\boldsymbol{Q}$ の場合についていうと，n と素な素数 p は非分岐で，(29)の対応で

$$\sigma_p \longleftrightarrow (p \bmod n)$$

とすれば，$p\boldsymbol{Z}$ の延長である $\boldsymbol{Q}(\zeta_n)$ の素イデアル P は σ_p-不変で，σ_p が mod P の剰余類の体に引き起こす同型がちょうどそのフロベニウス同型になっている（すなわち，アルチンの記号で $\sigma_p = \left(\dfrac{\boldsymbol{Q}(\zeta_n)/\boldsymbol{Q}}{p}\right)$．6.1；A 4.3, pp.147－148 参照)．このことから素イデアル (p) の $\boldsymbol{Q}(\zeta_n)$ における分解法則（A 4.3，定理 10）がえられる．一般の類体の場合にも同様な性質をもつ対応（アルチン写像）によってイデアル類群とガロア群の同型が与えられるのだ.」

C君「イデール群とはどう関係するのですか？」

私「まず，$\boldsymbol{Q}$ の場合のイデール群 $A_{\boldsymbol{Q}}^{\times}$ を定義しよう．すべての p に対する $\boldsymbol{Q}$ の完備化である p-進数体 $\boldsymbol{Q}_p$（補遺3)，それに実数体 $\boldsymbol{R} = \boldsymbol{Q}_{p_\infty}$ も加え，それらの乗法群の“制限直積”を考える：

(37) $$A_{\boldsymbol{Q}}^{\times} = \left(\prod_p{}' \boldsymbol{Q}_p^{\times}\right) \times \boldsymbol{R}^{\times}.$$

ここで，制限直積というのは

$$\prod_p{}' \boldsymbol{Q}_p^{\times} = \{\, (\alpha_p) \mid \forall' p \ \ |\alpha_p|_p = 1 \,\},$$

すなわち，通常の直積の中で，“ほとんどすべての”（すなわち，有限個を

除いてすべての）p に対して a_p が p-進単数（すなわち $\boldsymbol{Z}_p^\times$ の元）になっているような元（a_p）全体からなる部分群を考えるのだ．イデール群 $A_{\boldsymbol{Q}}^\times$ の中には確かに

(38) $$U = \left(\prod_p \boldsymbol{Z}_p^\times\right) \times \boldsymbol{R}_+^\times$$

が入っている．ただし $\boldsymbol{R}_+^\times$ は正の実数の乗法群を表す．イデール群の位相は次のように定義する．まず，U に通常の直積位相を入れる．そうすれば，U は（コンパクト群 $\prod_p \boldsymbol{Z}_p^\times$ と $\boldsymbol{R}_+^\times$ の直積だから）局所コンパクトアーベル群になる．次に，$A_{\boldsymbol{Q}}^\times$ には U が開部分群になるような位相を入れる．それによって，$A_{\boldsymbol{Q}}^\times$ も局所コンパクトアーベル群になる．

さて，$\boldsymbol{Q}$ の乗法群 $\boldsymbol{Q}^\times$ を対角的に $A_{\boldsymbol{Q}}^\times$ の中に埋め込むことができる．そうすると，$\boldsymbol{Z}$ が単項イデアル整域である（すなわち類数 1 である）ことから

$$A_{\boldsymbol{Q}}^\times = \boldsymbol{Q}^\times \cdot U$$

であることがいえる．一方，明らかに

$$\boldsymbol{Q}^\times \cap U = \{1\}.$$

よって，$\boldsymbol{Q}^\times$ は $A_{\boldsymbol{Q}}^\times$ の離散部分群になり，

(39) $$A_{\boldsymbol{Q}}^\times / \boldsymbol{Q}^\times \cong U$$

となる．したがって，“イデール類群” $A_{\boldsymbol{Q}}^\times / \boldsymbol{Q}^\times$ をその連結成分で割った商群は U の有限部分 $\prod_p \boldsymbol{Z}_p^\times$ と同型になる：

(39′) $$(A_{\boldsymbol{Q}}^\times / \boldsymbol{Q}^\times)/(\text{連結成分}) \cong \prod_p \boldsymbol{Z}_p^\times.$$

この両辺はそれぞれ（36′）の両辺の極限とみなすことができる.* そこで定理23の同型（35）と（39′）とを組み合わせれば，位相群としての同型

(40) $$\mathrm{Gal}\,(K/\boldsymbol{Q}) \cong (A_{\boldsymbol{Q}}^\times / \boldsymbol{Q}^\times)/(\text{連結成分})$$

がえられる．これは類体論の同型（29′）の極限であり，種々の法（導手）に対するイデアル類群の同型を一つにまとめたものとみなすことができる．

このようにイデール類群を考えると，類体論の同型をより簡明な形に述べることができる．これはシュヴァレー（C.Chevalley）の着想だ．イデール群の概念はその後代数群のアデール化として一般化され，現在では代数群の整数論，保型表現の理論などで欠くことのできない道具になっている．」

C君「虚数乗法論や岩沢理論のことも伺いたいのですが…」

私「あまり欲ばってはいけない．それはまたのお楽しみということにしよう．」

*　　*　　*

第6章　2次体 $\boldsymbol{Q}(\gamma)$ の整数論

この章では $\boldsymbol{Q}(\gamma)$（γ はガウスの和）の場合に限って，古典的な2次体の整数論について解説する．抽象代数的方法が整数論にいかに活用されるかを示すことと，3.9, 5.2で触れたガウスの和の話の結末（2次体の相互法則）を語ることがその目的である．一般の2次体の整数論*について，より詳しく知りたい方は高木［T1］，小野［O］などを参照して下さい．

6.1. 有限体 $\boldsymbol{F}_p$.　まず準備として，有限体 $\boldsymbol{F}_p$ について基本的なことをまとめておく．

5.2に述べたように，商環 $\boldsymbol{Z}/p\boldsymbol{Z}$ は体になる．これを $\boldsymbol{F}_p$ とかく．$\boldsymbol{F}_p$ においては

(1)
$$p\cdot 1 = \overbrace{1+\cdots+1}^{p} = 0$$

である．一般にこの式が成立するような体（より一般に1をもつ可換環）は“標数” p であるという．$\boldsymbol{F}_p$ を（部分体として）含む体は標数 p であるが，逆に標数 p の体 F は必ず $\boldsymbol{F}_p$ と同型な体を含み，$\boldsymbol{F}_p$ の拡大体と考られる．（同様のことが1をもつ可換環についてもいえる．）特に $F/\boldsymbol{F}_p$ が m 次（$m<\infty$）ならば，F は p^m 個の元からなる有限体になる．

標数 p の体 F では

(2)
$$(x+y)^p = x^p+y^p$$

が成立する．実際，二項係数

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \qquad (1 \leqq k \leqq p-1)$$

はすべて p で割り切れる（分子は p を含むが，分母は p で割れない）から，(2) の左辺を展開したとき，標数 p の体においては中間項が消えて右辺のようになる．この式により対応

(3) $$x \longmapsto x^p$$

は F の（体としての）自己準同型になることがわかる．（これを“フロベニウス（Frobenius）同型”という．）

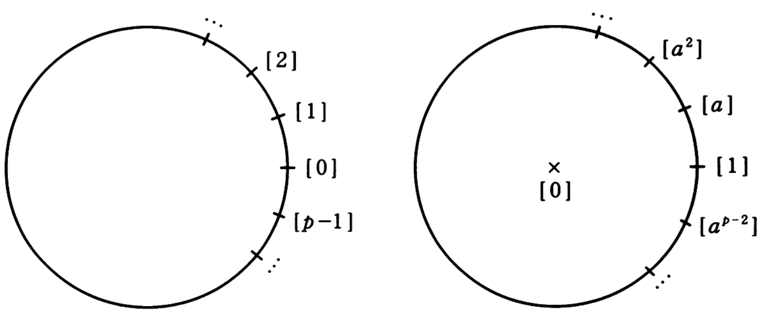
$F_p^\times$ は位数 $p-1$ のアーベル群であるから，すべての $a \in F_p^\times$ に対して

$$a^{p-1} = 1$$

が成立する．実際，この群は巡回群になる．すなわち，位数がちょうど $p-1$ になるような元（1の原始 $p-1$ 乗根，あるいは“原始根”）が存在する．たとえば，$p = 11$ のとき，[2] が原始根になる．実際，[2] のベキを作っていけば，

$$[2], [4], [8], [5], [10], [9], [7], [3], [6], [1], \cdots$$

となって，$p-1 = 10$ 個の既約剰余類がすべてえられる．またこれからわかるように，[8], [7], [6] も原始根である．



F_p の二つの顔

原始根の存在は次のように証明される．もし群 $F_p^\times$ が巡回群でないならば，アーベル群の基本定理（2.13，定理4）により

$$Z/a_1Z \times Z/a_2Z \qquad (a_1 | a_2,\ a_1 > 1)$$

の形の群と同型な部分群を含む．そのとき，$\boldsymbol{F}_p$ の中には方程式

$$x^{a_2}-1 = 0$$

の根が少なくとも a_1a_2（$>a_2$）個存在することになる．これは“一般に体においてn次方程式の根は高々 n 個しか存在しない”という定理に反する．

この同じ定理により，一般に標数 p の体 F の中で $\boldsymbol{F}_p$ の元は方程式

(4) $$x^p - x = 0$$

の根として，すなわちフロベニウス同型の“不動点”として，特徴づけられることがわかる．

上の考察の結果として，次の定理がえられる．

定理1（オイラーの規準）．奇素数 p に対して

(5) $$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

（証明） $p\equiv 1 \pmod 4$ のとき，またそのときに限り，$[-1]=(-1 \bmod p)$ が $\boldsymbol{F}_p$ において平方数であることを示せばよい．$G=\boldsymbol{F}_p^{\times}$ とおけば，G は位数 $p-1$ の巡回群であるから，3.4 の定理5により，位数 2 および $\dfrac{p-1}{2}$ の部分群 H_1, H_2 が（一意的に）存在する．明らかに，

$$H_1 = \{1, [-1]\}, \qquad H_2 = \{a^2 \mid a\in G\}$$

である．同じ定理により

$$4\,|\,p-1 \iff 2\,\Big|\,\frac{p-1}{2} \iff H_1\subset H_2$$

であるから，始めに述べた主張がえられる．　　　　（証終）

6.2. 2次体 $\boldsymbol{Q}(\gamma)$ の整数環．　一般に，代数的数 $\alpha\in\overline{\boldsymbol{Q}}$ はその（$\boldsymbol{Q}$ における）最小多項式が $\boldsymbol{Z}[x]$ に属するとき，**代数的整数**あるいは単に整数であるという．代数的整数全体の集合 $\mathcal{O}$ は加減乗の演算に関して閉じている，すなわち $\overline{\boldsymbol{Q}}$ の部分環になることが証明される．*（これは次の補題から容易に導かれる．$\alpha\in\overline{\boldsymbol{Q}}$ が整数になるためには，$\boldsymbol{Z}[\alpha]$ が $\boldsymbol{Z}$-加群として有限生成である

ことが必要十分である.）

代数体 F に対し，$\mathcal{O}_F = \mathcal{O} \cap F$ を "F の整数環" という．特に，$\mathcal{O}_{\boldsymbol{Q}} = \mathcal{O} \cap \boldsymbol{Q}$ は（定義から明らかなように）$\boldsymbol{Z}$ に等しい.

有限次代数体 F の整数環 $\mathcal{O}_F$ において，一般に素因数分解の一意性は成り立たず，イデアルは必ずしも単項でない．しかし，$\mathcal{O}_F$ の任意のイデアルは素イデアル（極大イデアル）の積に一意的に分解される．これがデデキント (Dedekind) によって証明された**イデアル論の基本定理** * である．（A 4.2，定理 6 参照）

一般に可換環 R の二つのイデアル A, B に対し，その積 AB は有限和 $\sum_i a_i b_i$ ($a_i \in A$, $b_i \in B$) 全体からなる集合として定義される．それはまた R のイデアルになる．これに関して明らかに，$AB = BA$, $(AB)C = A(BC)$, $A(B+C) = AB + AC$ などが成立する.

R のイデアル $P\ (\neq R)$ が "素" であるとは，$a, b \in R$ に対して

$$ab \in P \implies a \in P \text{ または } b \in P$$

が成立することをいう．P が "極大" であるとは，$P \neq R$ で，R のイデアル A に対して

$$P \subset A \implies A = P \text{ または } A = R$$

が成立することをいう．容易にわかるように，P が極大ならば，素である．またそのとき，商環 R/P は体になる．（以下，簡単のため，R の素イデアルというとき，$\{0\}$ と R は除外するものとする.）

イデアル論の基本定理が成立するような "整域"（1 をもち，零因子をもたない可換環）では，$\{0\}$ でないイデアルに関するこの二つの条件（素と極大）は同値になる．しかし，たとえば，$\boldsymbol{Z}[x]$ においてイデアル $2 \cdot \boldsymbol{Z}[x]$ や $x \cdot \boldsymbol{Z}[x]$ は素であるが極大ではない．$\boldsymbol{Z}[x]$ において，素元分解の一意性は成り立つが，イデアル論の基本定理は成立しないのである.

ここでは，われわれは一つの特別な例として 2 次体 $\boldsymbol{Q}(\gamma)$ の整数環を（一般論によらず直接に）考察する．ここに γ は（3.8 で定義した）ガウスの和

$$\gamma = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta_p^k \qquad (p \text{ は奇素数})$$

である．$\varepsilon = \left(\frac{-1}{p}\right)$ とおけば，（3.8 で述べたことと）定理 1 により

(6) $$\gamma^2 = \varepsilon p \equiv 1 \pmod 4$$

である．この章では $F=\boldsymbol{Q}(\gamma)$ の整数環を $R=\mathcal{O}_F$ とかくことにする．

定理 2.

(7) $$R = \{\, a+b\frac{1+\gamma}{2} \mid a, b \in \boldsymbol{Z} \,\}.$$

（証明）$\boldsymbol{Q}(\gamma)$ の任意の元 α は

$$\alpha = a + b\gamma, \qquad a, b \in \boldsymbol{Q}$$

と一意的にかける．$b=0$ ならば，明らかに $\alpha \in R \Rightarrow a \in R \cap \boldsymbol{Q} = \boldsymbol{Z}$ である．$b \neq 0$ ならば，α の最小多項式は

$$\begin{aligned} f(x) &= (x-a-b\gamma)(x-a+b\gamma) \\ &= x^2 - 2ax + a^2 - \varepsilon p b^2 \end{aligned}$$

であるから

(8) $$\alpha \in R \iff 2a,\ a^2 - \varepsilon p b^2 \in \boldsymbol{Z}.$$

（$\alpha = a+b\gamma$ に対して，$(a+b\gamma)(a-b\gamma) = a^2 - \varepsilon p b^2$ をその“ノルム”といい，$N\alpha$ とかく．$\mathrm{Gal}(F/\boldsymbol{Q}) = \{1, \sigma_0\}$ とすれば，$N\alpha = \alpha \cdot \alpha^{\sigma_0}$ である．）

いま（8）の右側の条件がみたされているとする．

1）　$a \in \boldsymbol{Z}$ ならば，明らかに $b \in \boldsymbol{Z}$ である．

2）　$a \notin \boldsymbol{Z}$ ならば，a, b を既約分数にかいたとき，分母は 2 であるから

$$a = \frac{1}{2} + a', \qquad b = \frac{1}{2} + b', \qquad a', b' \in \boldsymbol{Z}$$

の形になる．

逆に a, b がこの形ならば，（8）の（右側の）条件がみたされる．1）の場合は明らか．2）の場合も $2a \in \boldsymbol{Z}$ は明らか．

$$\begin{aligned} N\alpha = a^2 - \varepsilon p b^2 &= \frac{1}{4}\{(1+2a')^2 - \varepsilon p(1+2b')^2\} \\ &= \frac{1-\varepsilon p}{4} + (a'+a'^2) - \varepsilon p(b'+b'^2) \end{aligned}$$

は（6）により $\boldsymbol{Z}$ に属する．

以上により，$a+b\gamma$ が R に属するためには，a, b がともに整数であるか，ともに（整数ではない）半整数になるか，が必要十分である．これから（7）がえられる．　（証終）

定理2により，R は $\boldsymbol{Z}$ に $\frac{1+\gamma}{2}$ を添加してえられる環 $\boldsymbol{Z}[\frac{1+\gamma}{2}]$ である．$\frac{1+\gamma}{2}$ の最小多項式は

$$f_1(x) = x^2 - x + \frac{1-\varepsilon p}{4} \in \boldsymbol{Z}[x] \tag{9}$$

であるから，環の第2同型定理によって

$$R = \boldsymbol{Z}[\frac{1+\gamma}{2}] \cong \boldsymbol{Z}[x]/(f_1(x)\cdot\boldsymbol{Z}[x]) \tag{10}$$

が成立する．また R を加群（$\boldsymbol{Z}$-加群）と考えれば，

$$R = \boldsymbol{Z} \oplus \boldsymbol{Z}\cdot\frac{1+\gamma}{2} \cong \boldsymbol{Z}^2 \tag{11}$$

である．

6.3. R における極大イデアル.

$\boldsymbol{Q}(\gamma)$ の整数環 R における極大イデアルはどんなものだろうか？（デデキントの定理をみとめれば，素イデアルと極大イデアルは同義語になる．）

さて，Q を一つの極大イデアルとする．そのとき，$Q\cap\boldsymbol{Z}$ は明らかに $\boldsymbol{Z}$ の（0でない）イデアルであるから，ある正の整数 q があって，$Q\cap\boldsymbol{Z}=q\boldsymbol{Z}$ となる．（$\alpha\in Q$, $\alpha\neq 0$ をとれば，$N\alpha\in Q\cap\boldsymbol{Z}$, $N\alpha\neq 0$．よって $Q\cap\boldsymbol{Z}$ は確かに $\{0\}$ ではない．）環の第2同型定理により

$$\boldsymbol{Z}/q\boldsymbol{Z} \cong (Q+\boldsymbol{Z})/Q \subset R/Q$$

であるから，$\boldsymbol{Z}/q\boldsymbol{Z}$ は零因子をもたない環（整域）になる．したがって $q\boldsymbol{Z}$ は素イデアル，q は素数になる．逆に，素数 q に対して，$q\boldsymbol{Z}$ はもちろん $\boldsymbol{Z}$ の極大（素）イデアルであるが，その R への "延長" qR は R の（必ずしも極大でない）イデアルである．素数 q と R の極大イデアル Q に対して，次の3条

件は明らかに同値である：

$$Q \cap \boldsymbol{Z} = q\boldsymbol{Z} \iff q\boldsymbol{Z} \subset Q \iff qR \subset Q.$$

よって，R の極大イデアルを求めるには，素数 q から出発して，

$$qR \subset Q \subset R$$

となるような R のイデアル Q を調べれば十分である．

さて q を素数とすれば，自然な（環の）同型

$$\text{(12)} \qquad \boldsymbol{F}_q = \boldsymbol{Z}/q\boldsymbol{Z} \cong (\boldsymbol{Z}+qR)/qR \subset R/qR$$

が成立する．したがって，R/qR は標数 q の可換環である．R/qR を加群（または $\boldsymbol{F}_q$-加群，$\boldsymbol{F}_q$-ベクトル空間）と考えれば，（11）により

$$\text{(13)} \qquad R/qR = \boldsymbol{Z}/q\boldsymbol{Z} \oplus \boldsymbol{Z}/q\boldsymbol{Z}\cdot\left[\frac{1+\gamma}{2}\right]_q \cong \boldsymbol{F}_q \oplus \boldsymbol{F}_q.$$

ここに $[\cdots]_q$ は $\bmod qR$ の剰余類を表す．特に $|R/qR| = q^2$．

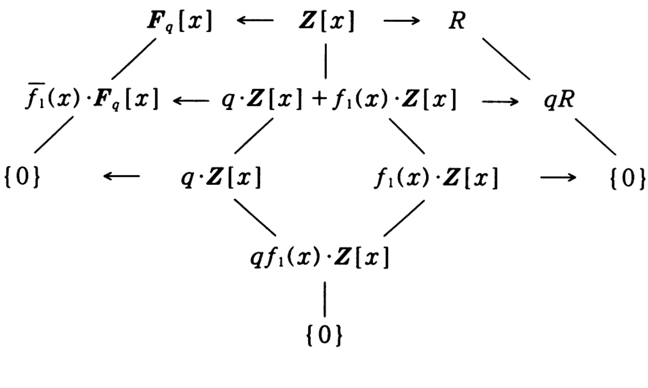
さて，$\dfrac{1+\gamma}{2}$ の最小多項式 $f_1(x) \in \boldsymbol{Z}[x]$ を $\bmod q\cdot\boldsymbol{Z}[x]$ で考えれば，$\boldsymbol{F}_q[x]$ の多項式

$$\text{(14)} \qquad \overline{f_1}(x) = x^2 - x + \left[\frac{1-\varepsilon p}{4}\right]_q$$

がえられる．

（10）により，次の図式が成立する：

(15)



この図式から（同型（12）の拡張として），自然な同型

$$(16)\qquad \boldsymbol{F}_q[x]/(\overline{f_1}(x)\cdot\boldsymbol{F}_q[x]) \xrightarrow{\sim} R/qR$$

$$(\,\bar{g}(x) \bmod \overline{f_1}(x)\cdot\boldsymbol{F}_q[x]\,) \longmapsto (\,g(\frac{1+\gamma}{2}) \bmod qR\,)$$

がえられる．ここに $g(x)\in\boldsymbol{Z}[x]$．

この同型により，qR を含むイデアル Q を求める問題は，$\overline{f_1}(x)$ の $\boldsymbol{F}_q[x]$ における因子を求める問題（２次式の因数分解）に帰着する．R や qR は標数0の世界の住人であるが，$\boldsymbol{F}_q$ や $\overline{f_1}(x)$ は標数 q の世界の住人である．より広い宇宙 $\boldsymbol{Z}[x]$ を媒介として，標数0の世界の問題が標数 q の世界のよりやさしい問題に移転されるのである．

6.4. 標数 q の２次式.

$q\neq 2$ のとき，$\boldsymbol{F}_q[x]$ の２次式について，（中学で習った）$\boldsymbol{R}[x]$ の２次式と全く同じことがいえる．（14）の $\overline{f_1}(x)$ についていえば，その判別式は $[\varepsilon p]_q$ であるから，$\overline{f_1}(x)$ の２根は

$$\frac{1}{2}(\,1\pm\sqrt{[\varepsilon p]_q}\,)$$

で与えられる．次の三つの場合が考えられる．

（I） $[\varepsilon p]_q$ が $\boldsymbol{F}_q$ で平方数でない，すなわち $\left(\frac{\varepsilon p}{q}\right)=-1$ のとき，$\overline{f_1}(x)$ は $\boldsymbol{F}_q$ に根をもたない，すなわち既約である．（これは実２次式が虚根をもつ場合に対応する．）

（II） $[\varepsilon p]_q\neq 0$ が $\boldsymbol{F}_q$ において平方数になる，すなわち $\left(\frac{\varepsilon p}{q}\right)=1$ のとき，$\overline{f_1}(x)$ は $\boldsymbol{F}_q$ において相異なる２根をもつ．実際，

$$a\in\boldsymbol{Z},\qquad \varepsilon p\equiv a^2 \pmod q$$

（必要ならば，a を $a+q$ でおきかえて，a は奇数としてよい）とすれば，

$$(17)\qquad \overline{f_1}(x) = \left(x-[\frac{1+a}{2}]_q\right)\left(x-[\frac{1-a}{2}]_q\right).$$

（これは実2次式が二つの実根をもつ場合に対応する．）

(III)　$[\varepsilon p]_q = 0$，すなわち $q = p$ のとき，$\overline{f_1}(x)$ は $\boldsymbol{F}_q$ において重根をもつ．実際，

$$\overline{f_1}(x) = \left(x - [\tfrac{1}{2}]_q\right)^2. \tag{18}$$

（これは実2次式が重根をもつ場合に対応する．）

$q = 2$ のときは少し様子が異なる．

(I′)　$\dfrac{1-\varepsilon p}{4} \equiv 1 \pmod 2$，すなわち

$$p \equiv 3 \text{ または } 5 \pmod 8$$

のとき，$\overline{f_1}(x) = x^2+x+1$ は $\boldsymbol{F}_2 = \{0, 1\}$ に根をもたない，すなわち既約である．

(II′)　$\dfrac{1-\varepsilon p}{4} \equiv 0 \pmod 2$，すなわち

$$p \equiv 1 \text{ または } 7 \pmod 8$$

のとき，$\overline{f_1}(x) = x^2+x$ は $\boldsymbol{F}_2$ において相異なる2根 0, 1 をもつ．

0次式	$\mathbf{1}$
1次式	$\boldsymbol{x}$, $\boldsymbol{x+1}$
2次式	x^2, x^2+1, x^2+x, $\boldsymbol{x^2+x+1}$
3次式	x^3, x^3+1, x^3+x, $\boldsymbol{x^3+x+1}$ x^3+x^2, $\boldsymbol{x^3+x^2+1}$, x^3+x^2+x, x^3+x^2+x+1
…	………

$\boldsymbol{F}_2[x]$ の多項式（太字は既約多項式）

以上 $\overline{f_1}(x)$ の分解に応じて，qR の分解の仕方がわかる．

(I), (I′) の場合：$\boldsymbol{F}_q[x]/(\overline{f_1}(x)\boldsymbol{F}_q[x])$ は体になる．よって (16) により R/qR も体になる．（それは $\boldsymbol{F}_q$ の2次拡大 $\boldsymbol{F}_q(\sqrt{[\varepsilon p]_q})$ である．）したがって qR 自身が極大イデアルである．

この場合，（素イデアル）$q\boldsymbol{Z}$ は R において“分解しない”という．

(II), (II′) の場合： 可換環としての同型

$$\boldsymbol{F}_q[x]/(\overline{f_1}(x)\boldsymbol{F}_q[x]) \cong \boldsymbol{F}_q \oplus \boldsymbol{F}_q \tag{19}$$

が成り立つ．実際，(II) の場合には

$$e_1 = \left([a]_q^{-1}(x-[\frac{1-a}{2}]_q) \bmod \overline{f_1}(x)\boldsymbol{F}_q[x]\right)$$

$$e_2 = \left(-[a]_q^{-1}(x-[\frac{1+a}{2}]_q) \bmod \overline{f_1}(x)\boldsymbol{F}_q[x]\right)$$

とおけば，簡単な計算により

$$e_1+e_2 = 1, \qquad e_1e_2 = 0,$$

したがって，$e_1^2=e_1$, $e_2^2=e_2$ も成立し，e_1, e_2 はこの環における“1の分解”を与える．よって $R'=\boldsymbol{F}_q[x]/(\overline{f_1}(x)\boldsymbol{F}_q[x])$ とおけば，環の直和分解

$$R' = R'e_1 \oplus R'e_2, \qquad R'e_i = \boldsymbol{F}_q e_i \cong \boldsymbol{F}_q$$

が成立し，(19) がえられる．(II′) の場合には

$$e_1 = (x \bmod \overline{f_1}(x)\boldsymbol{F}_2[x]),$$

$$e_2 = (x+1 \bmod \overline{f_1}(x)\boldsymbol{F}_2[x])$$

とおけばよい．

(16) の同型により

$$\boldsymbol{F}_q e_i \longleftrightarrow Q_i/qR.$$

ここに，Q_i は R のイデアルで，

$$Q_1+Q_2 = R, \qquad Q_1 \cap Q_2 = qR$$

をみたす．したがって，$Q_1Q_2=qR$ となる．また容易にわかるように，$Q_2=Q_1^{\sigma_0}$ である．

一般に，$\alpha_1, \cdots, \alpha_r \in R$ が生成する R のイデアル $\sum_{i=1}^{r} R\alpha_i$ を，簡単のため $(\alpha_1, \cdots, \alpha_r)$ とかくことにする．(16) の対応により Q_i を実際に計算すれば，(II) の場合には

$$Q_1 = (q, \frac{a+\gamma}{2}), \qquad Q_2 = (q, \frac{a-\gamma}{2}), \tag{20}$$

(II′) の場合には

$$Q_1 = \left(2, \frac{1+\gamma}{2}\right), \qquad Q_2 = \left(2, \frac{1-\gamma}{2}\right) \tag{20′}$$

となる.

この場合, $q\boldsymbol{Z}$ は R において“分解する”という.

(III) の場合： $Q=\gamma R$ とおけば, 明らかに

$$pR \subset Q \subset R, \qquad pR = Q^2, \qquad Q^{\sigma_0} = Q$$

である.

この場合, $p\boldsymbol{Z}$ は R において“分岐する”という.

以上を要約すれば, 次の定理がえられる.

定理 3. R を $\boldsymbol{Q}(\gamma)$ の整数環とする.

1) $q \neq 2, p$ のとき,

$\left(\dfrac{\varepsilon p}{q}\right) = 1$ ならば, $q\boldsymbol{Z}$ は R で分解する.

$\left(\dfrac{\varepsilon p}{q}\right) = -1$ ならば, $q\boldsymbol{Z}$ は R で分解しない.

2) $q=2$ のとき,

$p \equiv 1$ または 7 (mod 8) ならば, $2\boldsymbol{Z}$ は R で分解する.

$p \equiv 3$ または 5 (mod 8) ならば, $2\boldsymbol{Z}$ は R で分解しない.

3) $q=p$ のとき, $p\boldsymbol{Z}$ は R で分岐する.

6.5. 素イデアル分解の例.

例 1 : $\boldsymbol{Q}(\sqrt{5})$.

$$\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1, \qquad \left(\frac{5}{7}\right) = -1, \qquad \left(\frac{5}{11}\right) = 1$$

であるから, $2\boldsymbol{Z}$, $3\boldsymbol{Z}$, $7\boldsymbol{Z}$ は分解しない. $11\boldsymbol{Z}$ は分解する. 目算でわかるように

$$11 = \frac{7+\sqrt{5}}{2}\cdot\frac{7-\sqrt{5}}{2}$$

であるから，

$$(11) = Q_1Q_2, \qquad Q_1 = \left(\frac{7+\sqrt{5}}{2}\right), \quad Q_2 = \left(\frac{7-\sqrt{5}}{2}\right).$$

この場合，R は P.I.D.（単項イデアル整域）になることが証明される.* したがって，一般に奇素数 q に対して，$q\boldsymbol{Z}$ が R で分解することと 2 次不定方程式

$$x^2 - 5y^2 = 4q$$

が整数解をもつこととは同値である.（次節で述べるように，相互法則により $\left(\frac{5}{q}\right) = \left(\frac{q}{5}\right)$ であるから，この条件は $q \equiv \pm 1 \pmod 5$ と同値である.）

またこの場合，単数群 $R^\times$ は $\rho = \frac{1+\sqrt{5}}{2}$ で生成される無限巡回群と $\{\pm 1\}$ の直積になる．実際，$\alpha = \frac{a+b\sqrt{5}}{2} \in R$ に対し

$$\alpha \in R^\times \iff N\alpha = \alpha\alpha^{\sigma_0} = \frac{a^2-5b^2}{4} = \pm 1$$

であるから，R の単数を求める問題はいわゆる “ペル方程式”

$$(*) \qquad x^2 - 5y^2 = \pm 4$$

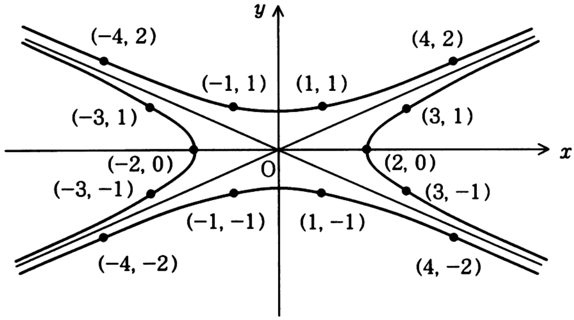
の整数解（すなわち（＊）で定義される二つの双曲線上の格子点）を求める問題に帰着する．次ページの図からわかるように，それは

$$\frac{x+y\sqrt{5}}{2} = \pm\left(\frac{1+\sqrt{5}}{2}\right)^m \qquad (m = 0, \pm 1, \pm 2, \cdots)$$

によって与えられる解

$$(x, y) = (\pm 2, 0), (\pm 3, \pm 1), (\pm 7, \pm 3), \cdots,$$
$$(\pm 1, \pm 1), (\pm 4, \pm 2), (\pm 11, \pm 5), \cdots$$

によって尽くされている.



$x^2-5y^2=\pm 4$ のグラフ

例 2 : $\boldsymbol{Q}(\sqrt{-3})$.

$$\left(\frac{-3}{5}\right)=-1,\quad \left(\frac{-3}{7}\right)=\left(\frac{4}{7}\right)=1,\quad \left(\frac{-3}{11}\right)=\left(\frac{8}{11}\right)=-1$$

であるから，$2\boldsymbol{Z}$, $5\boldsymbol{Z}$, $11\boldsymbol{Z}$ は分解しない．$7\boldsymbol{Z}$ は分解する．

$$7=(2+\sqrt{-3})(2-\sqrt{-3})$$

であるから，

$$(7)=Q_1Q_2,\quad Q_1=(2+\sqrt{-3}),\ Q_2=(2-\sqrt{-3}).$$

この場合にも，R は P.I.D. である.* $R^\times$ は $\zeta_6=\dfrac{1+\sqrt{-3}}{2}$ によって生成される位数 6 の巡回群である．

一般に，実 2 次体の単数群は $\{\pm 1\}\times\{\rho^k\ (k\in\boldsymbol{Z})\}$ の形の無限群になり，虚 2 次体の単数群は有限巡回群で，$\boldsymbol{Q}(\sqrt{-1})$, $\boldsymbol{Q}(\sqrt{-3})$ の場合を除き，$\{\pm 1\}$ になることが知られている．$\boldsymbol{Q}(\sqrt{-1})$ の場合には，位数 4 の巡回群 $\{\pm 1,\pm\sqrt{-1}\}$ である．一般の有限次代数体の単数群の構造は“ディリクレ（Dirichlet）の単数定理”* によって与えられる．

例 3 : $\boldsymbol{Q}(\sqrt{-23})$.

$$\left(\frac{-23}{3}\right)=\left(\frac{1}{3}\right)=1,\quad \left(\frac{-23}{5}\right)=\left(\frac{2}{5}\right)=-1,$$

$$\left(\frac{-23}{7}\right)=\left(\frac{5}{7}\right)=-1,\quad -23\equiv 1\pmod 8$$

であるから，$2\boldsymbol{Z}$，$3\boldsymbol{Z}$ は分解し，$5\boldsymbol{Z}$，$7\boldsymbol{Z}$ は分解しない．R において（20′），（20）により

$$(2) = P_1P_2, \quad P_1 = \left(2, \frac{1+\sqrt{-23}}{2}\right), \quad P_2 = \left(2, \frac{1-\sqrt{-23}}{2}\right),$$

$$(3) = Q_1Q_2, \quad Q_1 = \left(3, \frac{1+\sqrt{-23}}{2}\right), \quad Q_2 = \left(3, \frac{1-\sqrt{-23}}{2}\right).$$

簡単なイデアル計算からわかるように

$$P_1^3 = \left(\frac{3-\sqrt{-23}}{2}\right), \quad Q_1^3 = (2-\sqrt{-23}),$$

$$P_1Q_1 = \left(\frac{1+\sqrt{-23}}{2}\right), \quad P_2Q_2 = \left(\frac{1-\sqrt{-23}}{2}\right)$$

等が成立する．この場合，$\boldsymbol{Q}(\sqrt{-23})$ の“イデアル類群”は（たとえば P_1 の類から生成される）位数 3 の巡回群になる．したがって，素元分解の一意性は成り立たない．たとえば

$$6 = 2\cdot 3 = \frac{1+\sqrt{-23}}{2}\cdot\frac{1-\sqrt{-23}}{2}$$

のように 6 は 2 通りの素元分解をもつ．しかし素イデアルまでいけば

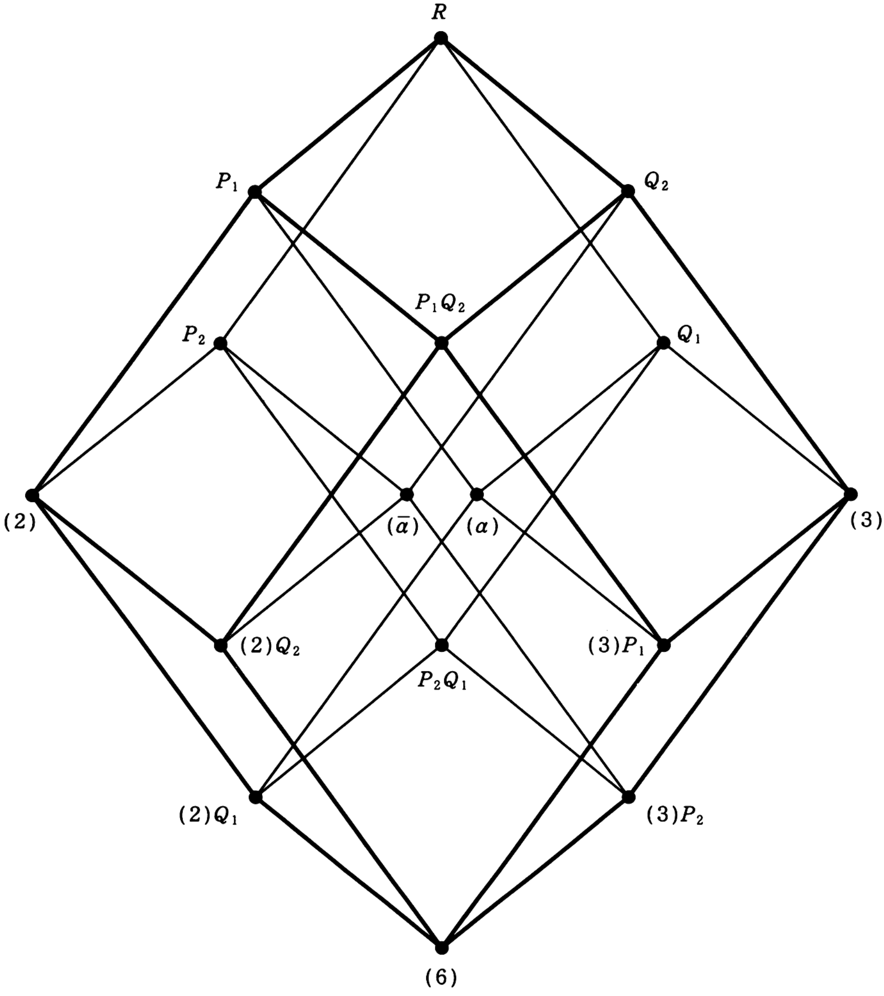
$$(6) = P_1P_2Q_1Q_2$$

が（6）の唯一の素イデアル分解である（次ページの図参照）．

一般に有限次代数体 F で二つのイデアル A, B は，ある $\alpha \in F^\times$ があって，$A = (\alpha)B$ となるとき，同値であるといい，$A \sim B$ とかく．この同値類をイデアル類という．イデアル類は乗法に関して群になる．（これは $\mathcal{O}_F$ の分数イデアルの群を単項イデアルの作る部分群で割った商群と同じである．A 4.2 参照．）これを F の**イデアル類群**，その位数を F の**類数**といい，通常 h で表す．一般に有限次代数体に対して $h < \infty$ であることが知られている.* $R = \mathcal{O}_F$ が P.I.D. になるときには，$h = 1$ であるが，上の $\boldsymbol{Q}(\sqrt{-23})$ では $h = 3$ で，

$$P_1^2 \sim P_2 \sim Q_1 \sim Q_2^2$$

となっている．類数（またはイデアル類群）は整数環 R が P.I.D. とどれだけ異なっているかを示す非常に重要な不変量である．



$$\alpha=\frac{1+\sqrt{-23}}{2}$$

$\boldsymbol{Q}(\sqrt{-23})$ における 6 の約数（イデアル）

例4：$\boldsymbol{Q}(\sqrt{-15})$．この場合，$15=3\cdot5$ は合成数であるが，$-15\equiv1 \pmod 4$ であるから，上に述べたことはほとんどそのまま成立する．（“応用問題”として考えてみて下さい．） $\boldsymbol{Q}(\sqrt{-15})$ の整数環は

$$R=\boldsymbol{Z}\left[\frac{1+\sqrt{-15}}{2}\right]$$

である．判別式は -15 で，$3\boldsymbol{Z}$ と $5\boldsymbol{Z}$ が R で分岐する：

$$(3)=(3,\sqrt{-15})^2,\qquad (5)=(5,\sqrt{-15})^2.$$

また

$$\left(\frac{-15}{7}\right)=\left(\frac{-15}{11}\right)=-1,\qquad -15\equiv1 \pmod 8$$

であるから，$2\boldsymbol{Z}$ は分解し，$7\boldsymbol{Z}$，$11\boldsymbol{Z}$ は分解しない．

$$(2)=\left(2,\frac{1+\sqrt{-15}}{2}\right)\cdot\left(2,\frac{1-\sqrt{-15}}{2}\right).$$

この場合，$\boldsymbol{Q}(\sqrt{-15})$ の類数は 2 で，素元分解の一意性は成り立たない．たとえば

$$4=2^2=\frac{1+\sqrt{-15}}{2}\cdot\frac{1-\sqrt{-15}}{2}.$$

例5：$\boldsymbol{Q}(\sqrt{-5})$．この場合 $-5\equiv3 \pmod 4$ であるから，上に扱ったカテゴリーには入らないが，比較のために結果だけをかいておこう．

$\boldsymbol{Q}(\sqrt{-5})$ の整数環は

$$R=\boldsymbol{Z}[\sqrt{-5}]=\{a+b\sqrt{-5}\mid a,b\in\boldsymbol{Z}\}$$

で与えられる．$\sqrt{-5}$ の $\boldsymbol{Q}$ における最小多項式は $f(x)=x^2+5$，その判別式は $-20=-4\cdot5$ である．したがって，$2\boldsymbol{Z}$，$5\boldsymbol{Z}$ が分岐する：

$$(2)=(2,1+\sqrt{-5})^2,\qquad (5)=(\sqrt{-5})^2.$$

素数 $q\neq2,5$ は $\left(\frac{-5}{q}\right)=1$ のとき，そのときに限り R において分解する．たとえば $\left(\frac{-5}{3}\right)=1$ であるから，$3\boldsymbol{Z}$ は R において

$$(3) = (3, 1+\sqrt{-5})\cdot(3, 1-\sqrt{-5})$$

と分解する．$\boldsymbol{Q}(\sqrt{-5})$ の類数は2で，この場合にも6は2通りの素元分解

$$6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

をもつ．

6.6. 2次体の相互法則.　ここまでの議論はいわば純代数的で，$\gamma=\sqrt{\varepsilon p}$ がガウスの和であることは別に使っていない．（したがって，それは原則的にはどんな有限次代数体にも適用できる．）しかしここで5.2で述べたことを思い出してみよう．2次体 $\boldsymbol{Q}(\gamma)$ は円分体 $\boldsymbol{Q}(\zeta_p)$ に含まれている．$\sigma\in \mathrm{Gal}(\boldsymbol{Q}(\zeta_p)/\boldsymbol{Q})$ に対し $1\leqq k(\sigma)\leqq p-1$ が定まり，

$$\zeta_p^{\sigma} = \zeta_p^{k(\sigma)}$$

が成立し，この対応 $\sigma\to[k(\sigma)]_p$ により

$$\mathrm{Gal}(\boldsymbol{Q}(\zeta_p)/\boldsymbol{Q}) \cong (\boldsymbol{Z}/p\boldsymbol{Z})^{\times} = \boldsymbol{F}_p^{\times}$$

となるのであった（5.2の（29））．

いま q を p と異なる素数とし，$k(\sigma)\equiv q \pmod p$ となるような σ を σ_q とかくことにする．そのとき

$$\gamma^{\sigma_q} = \left(\frac{q}{p}\right)\gamma \tag{21}$$

が成り立つ．したがって

$$\sigma_q|\boldsymbol{Q}(\gamma) = 1 \iff \left(\frac{q}{p}\right) = 1$$

である（5.2の（30））．

σ_q は $\boldsymbol{Q}(\gamma)$ の整数環 R を不変にする．したがって，イデアル qR をも不変にし，商環 R/qR の自己同型 $\bar{\sigma}_q$ を引き起こす．

定理4. q を p と異なる素数とすれば，σ_q によって R/qR に引き起こされる自己同型 $\bar{\sigma}_q$ は R/qR のフロベニウス同型と一致する．

（証明）$R/qR=\boldsymbol{F}_q[[\frac{1+\gamma}{2}]_q]$ であるから，$[\frac{1+\gamma}{2}]_q$ に対する作用が一致

することを見ればよい．γ の定義式および等式 $\sum_{k=0}^{p-1}\zeta_p{}^k=0$ から，

$$\frac{1+\gamma}{2} = 1+\sum_{k=1}^{p-1}\left(\frac{1}{2}\left(1+\left(\frac{k}{p}\right)\right)\zeta_p{}^k\right)\ (\in \boldsymbol{Z}[\zeta_p])$$

とかくことができる．$\zeta_p{}^{\sigma_q}=\zeta_p{}^q$ であるから，この式から

$$[\frac{1+\gamma}{2}]_q^{\bar{\sigma}_q} = [\frac{1+\gamma}{2}]_q^q$$

がえられる．（証終）

系．q を p と異なる素数とするとき，次の三つの条件は同値である．

（i） $\sigma_p|\boldsymbol{Q}(\gamma) = 1$.

（ii） R/qR のフロベニウス同型は恒等写像になる．

（iii） R/qR は体でない．

（証明） (i) ⇒ (ii) は定理4から明白．一般に（21）により

$$[\frac{1+\gamma}{2}]_q^{\bar{\sigma}_q} = [\frac{1}{2}\left(1+\left(\frac{q}{p}\right)\gamma\right)]_q$$

であるから，逆に

$$\text{(ii)} \implies \left(\frac{q}{p}\right)=1 \implies \text{(i)}$$

である．前節で述べたように

$$R/qR \cong \begin{cases} \boldsymbol{F}_q(\sqrt{[\varepsilon p]_q}) & (q\boldsymbol{Z}\text{ が分解しないとき}) \\ \boldsymbol{F}_q \oplus \boldsymbol{F}_q & (q\boldsymbol{Z}\text{ が分解するとき}) \end{cases}$$

であるから，R/qR のフロベニウス同型は R/qR が体でないとき，またそのときに限って，恒等写像になる．よって (ii) ⇔ (iii) である．（証終）

前節の結果，上の系，および（21）により，$q\neq 2, p$ に対して

(22)
$$\left(\frac{\varepsilon p}{q}\right)=1 \iff q\boldsymbol{Z}\text{ が }R\text{ で分解する}$$
$$\iff \left(\frac{q}{p}\right)=1.$$

$q=2$ のときも同様にして

(23)
$$\varepsilon p \equiv 1 \pmod 8 \iff 2\boldsymbol{Z} \text{ が } R \text{ で分解する}$$
$$\iff \left(\frac{2}{p}\right) = 1.$$

このように，素イデアル $q\boldsymbol{Z}$ の R（$\boldsymbol{Q}(\sqrt{\varepsilon p})$ の整数環）における分解法則が，q の p を法とする剰余類によって決定される．これが**2次体の相互法則**である．

(22), (23) の関係を（定理1を使って）かき直せば，いわゆる“平方剰余の相互法則”

(24)
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

(25)
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

がえられる（ただし p, q は相異なる奇素数を表す）．

たとえば，$\left(\frac{5}{q}\right) = \left(\frac{q}{5}\right)$ であるから，$q\boldsymbol{Z}$ の $\boldsymbol{Q}(\sqrt{5})$ における分解法則は $q \bmod 5$ で決まる．しかし

$$\left(\frac{-5}{q}\right) = (-1)^{\frac{q-1}{2}}\left(\frac{q}{5}\right)$$

であるから，$\boldsymbol{Q}(\sqrt{-5})$ における分解法則は $q \bmod 20$ で決まる．これは $\boldsymbol{Q}(\sqrt{-5})$ が $\boldsymbol{Q}(\zeta_5)$ でなく，$\boldsymbol{Q}(\zeta_{20})$ に含まれることを反映している．（pp. 152−153 の図参照）

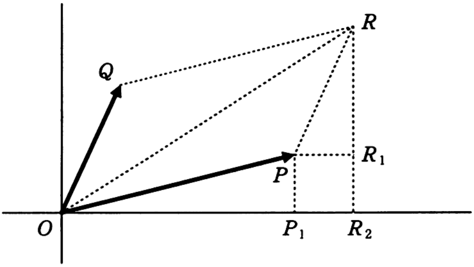
ガウスが炯眼（けいがん）にも見抜いていたように，平方剰余の相互法則は2次体や円分体の整数論に深く関わっているのである．

補遺1. 行列式 $\det(A) = ad - bc$ について

A 1.1. 行列式の幾何学的意味. $\boldsymbol{R}^2$ における 0 でない二つのベクトル

$$\overrightarrow{OP} = \begin{pmatrix} a \\ c \end{pmatrix}, \quad \overrightarrow{OQ} = \begin{pmatrix} b \\ d \end{pmatrix}$$

が正の向きに位置しているとき（すなわち，OPQ の順序がこの三角形の内部を左に見る向きになっているとき），$\det(A) = ad - bc$ は平行四辺形 $OPRQ$ の面積を表す.



実際，図において

$$\triangle OP_1P = \frac{1}{2}ac,$$

$$\triangle OR_2R = \frac{1}{2}(a+b)(c+d),$$

$$\triangle PR_1R = \frac{1}{2}bd,$$

$$\square P_1R_2R_1P = bc$$

であるから，

$$\triangle OPR = \frac{1}{2}(a+b)(c+d) - \frac{1}{2}ac - \frac{1}{2}bd - bc$$
$$= \frac{1}{2}(ad-bc).$$

よって，平行四辺形 $OPRQ$ の面積は $ad-bc$ になる．

ベクトル $\overrightarrow{OP}$, $\overrightarrow{OQ}$ が平行のときには，$a:c=b:d$ であるから，$ad-bc=0$ となる．

ベクトル $\overrightarrow{OP}$, $\overrightarrow{OQ}$ が負の向きに位置しているときには，$\overrightarrow{OQ}$, $\overrightarrow{OP}$ は正の向きに位置している．よって上の結果により，$ad-bc<0$ で，平行四辺形 $OPRQ$ の面積はその絶対値 $|ad-bc|$ で与えられる．

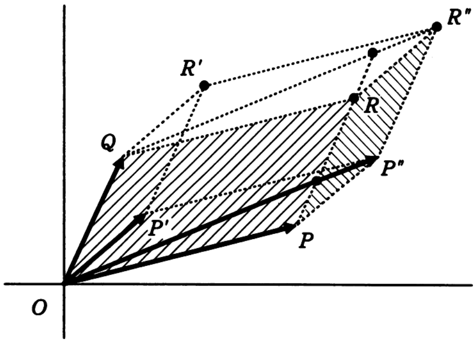
行列式の性質

(1) $$\det\begin{pmatrix} a+a' & b \\ c+c' & d \end{pmatrix} = \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \det\begin{pmatrix} a' & b \\ c' & d \end{pmatrix}$$

は，下の図から読みとることができる．この図では

$$\overrightarrow{OP} = \begin{pmatrix} a \\ c \end{pmatrix}, \quad \overrightarrow{OP'} = \begin{pmatrix} a' \\ c' \end{pmatrix}, \quad \overrightarrow{OP''} = \begin{pmatrix} a+a' \\ c+c' \end{pmatrix}, \quad \overrightarrow{OQ} = \begin{pmatrix} b \\ d \end{pmatrix}$$

である．平行四辺形 $OP''R''Q$ の面積が平行四辺形 $OPRQ$, $PP''R''R$ の面積の和になることを見ればよいが，それは図から明白であろう．



A 1.2. 行列式の群論的意味.

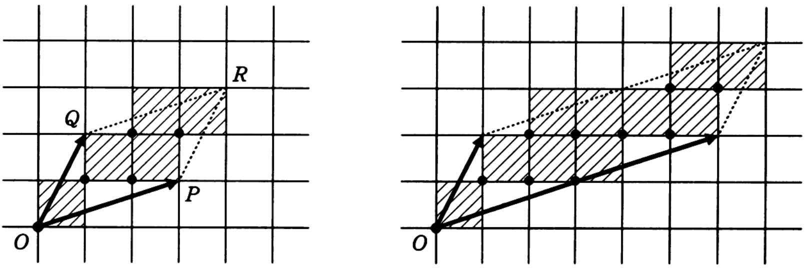
成分が整数であるようなベクトルを**整ベクトル**ということにする．整ベクトル $\begin{pmatrix} a \\ c \end{pmatrix}$ は a, c が互いに素であるとき（す

なわち，a, c の最大公約数が 1 であるとき）**原始的**であるという．ベクトル $\overrightarrow{OP}$ が原始的であるためには，線分 OP の上に端点 O, P 以外に格子点（座標が整数であるような点）が存在しないことが必要十分である．

ベクトル $\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix}$ がともに原始的であるとき，平行四辺形 $OPRQ$ の内部に含まれる格子点の数を N とすれば，

(2) $$\det(A) = ad - bc = N + 1$$

が成立する．下の図（左）を見てその理由を考えて下さい．



この図の場合には，

$$A = \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix}, \quad N = 4, \quad \det(A) = 5$$

である．

一般に（周囲まで含めた）平行四辺形 $OPRQ$ から辺の（閉）線分 PR, QR を取り去った残りの部分は，二つのベクトル $\overrightarrow{OP}$, $\overrightarrow{OQ}$ から生成される平行移動の群（それは $\cong A\boldsymbol{Z}^2$）の“基本領域”である．$\overrightarrow{OP}$, $\overrightarrow{OQ}$ が整ベクトルであるとき，上の考察からわかるように，この基本領域の中に含まれる格子点の個数は $\det(A)$ に等しい．（上図（右）の場合には $\det(A) = 10$ である．）一方，これらの格子点の全体は商群 $\boldsymbol{Z}^2/A\boldsymbol{Z}^2$ の代表系になっている．よって

(3) $$|\boldsymbol{Z}^2/A\boldsymbol{Z}^2| = \det(A)$$

という関係がえられる．この関係式は単因子論からもえられる (2.13参照)．

補遺 2. 体の同型の拡張

A 2.1. 素朴な証明. 4.7 の定理 13 を再記する.

定理 4.13. F_1, F_2 を二つの代数体とし,(体の) 同型 $\sigma_0 : F_1 \xrightarrow{\sim} F_2$ が与えられたとする. そのとき, ある $\sigma \in G = \mathrm{Aut}(\overline{\boldsymbol{Q}})$ があって $\sigma|F_1 = \sigma_0$ となる.

素朴に考えれば, この定理は次のように証明される.

まず $\overline{\boldsymbol{Q}}$ の元の個数は可付番だから, 数列 $\alpha_1, \alpha_2, \cdots \in \overline{\boldsymbol{Q}}$ があって,

$$\overline{\boldsymbol{Q}} = \boldsymbol{Q}(\alpha_1, \alpha_2, \cdots)$$

となる. いま

$$K_0 = F_1, \qquad K_n = F_1(\alpha_1, \cdots, \alpha_n) \quad (n = 1, 2, \cdots)$$

とおけば,

$$(1) \qquad K_0 \subset K_1 \subset K_2 \subset \cdots, \qquad \bigcup_{n=1}^{\infty} K_n = \overline{\boldsymbol{Q}}$$

となる. そこで同型 $\sigma_0 : K_0 \to \text{into } \overline{\boldsymbol{Q}}$ から出発して, それを次々に同型

$$\sigma_n : K_n \to \text{into } \overline{\boldsymbol{Q}} \qquad (n = 1, 2, \cdots)$$

に拡張してゆけば, 求める $\sigma \in \mathrm{Aut}(\overline{\boldsymbol{Q}})$ がえられるであろう. いま σ_0 から出発して σ_n まで拡張できたとする. そのとき $K_n' = K_n^{\sigma_n}$ とし, α_{n+1} の K_n における最小多項式 $f_n(x)$ $(\in K_n[x])$ の係数に σ_n を施してえられる (K_n' の) 多項式を $f_n^{\sigma_n}(x)$ とすれば, σ_n の自然な拡張である同型

$$\sigma_{n+1}' : K_n[x]/(f_n(x)) \longrightarrow K_n'[x]/(f_n^{\sigma_n}(x))$$

がえられる. $f_n^{\sigma_n}(x)$ の一つの根を β_{n+1} とすれば, 4.7 の定理 12 により自然な同型

$$K_n[x]/(f_n(x)) \cong K_n(\alpha_{n+1}) = K_{n+1},$$

$$K_n'[x]/(f_n^{\sigma_n}(x)) \cong K_n'(\beta_{n+1}) = K_{n+1}'$$

がえられる．これらの同型を合成すれば，σ_n の拡張である同型

(2) $$\sigma_{n+1} : K_{n+1} \longrightarrow K_{n+1}' \subset \overline{\boldsymbol{Q}}$$

$$\sigma_{n+1}|K_n = \sigma_n, \qquad \sigma_{n+1}(\alpha_{n+1}) = \beta_{n+1}$$

がえられる．これで帰納的定義は完成した．

さて，任意の $\alpha \in \overline{\boldsymbol{Q}}$ をとれば，ある n があって $\alpha \in K_n$．よって，

$$\sigma(\alpha) = \sigma_n(\alpha)$$

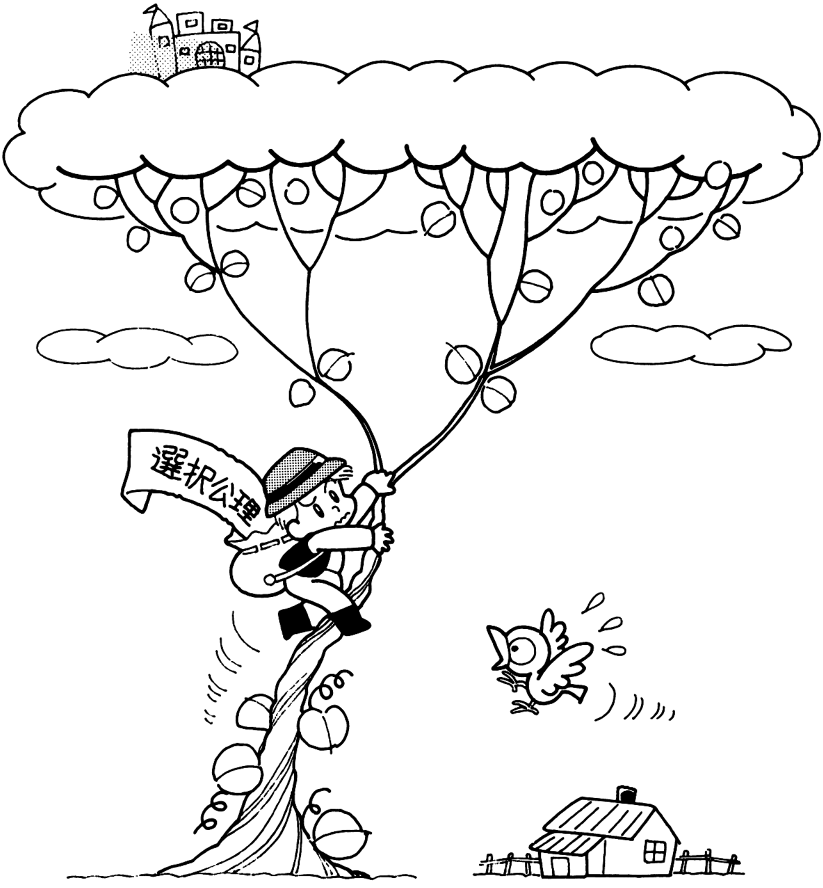
によって σ を定義すれば，容易にわかるように，それは well-defined で（すなわち n のとり方によらず定まり）$\overline{\boldsymbol{Q}}$ からそれ自身の中への同型になる．しかし $\sigma(\overline{\boldsymbol{Q}}) \cong \overline{\boldsymbol{Q}}$ であるから，$\boldsymbol{Q}[x]$ の任意の n 次既約多項式は $\sigma(\overline{\boldsymbol{Q}})$ の中に n 個の根をもつ．よって実は $\sigma(\overline{\boldsymbol{Q}}) = \overline{\boldsymbol{Q}}$ となる．したがって $\sigma \in \mathrm{Aut}(\overline{\boldsymbol{Q}})$ である．（証終）

読者はこの証明で満足されるだろうか？ 厳密にいうと，同型の列

(3) $$\sigma_1, \sigma_2, \cdots$$

を帰納的に定義するところに問題がある．一つの与えられた自然数 n に対して，同型の有限列 $\sigma_1, \sigma_2, \cdots, \sigma_n$ を上の方法で定義することに問題はない．しかし σ を定義するためには，(3) の無限列が定義されていなければならない．上の証明では，σ_{n+1} を定義するためには $f_n^{\sigma_n}(x)$ のいくつかある根の中からその一つ β_{n+1} を選ばねばならない．そして，無限個の n に対するこのような選択が全部完了していると仮定しなければならない．このような仮定を実現するためには“選択公理”を使う必要がある．

選択公理にはいくつかの同値な formulation が可能であるが，その中でよく使われるのがツォルン（Zorn）の補題である．（チコノフの定理もその一つである．）次節でツォルンの補題を述べ，A2.3 でそれを使う証明（本質的には上の証明と同じであるが）を述べることにする．



ジャック少年豆の木を登る．彼は果して天まで登れるだろうか？

A 2.2.　ツォルンの補題．　まず半順序集合に関するいくつかの定義を述べる．

集合 A の二つの元に対する関係 $a \leq b$ が次の条件をみたすとき，**半順序** といい，半順序の定義された集合を半順序集合という．

（i）　$\forall a \in A$ に対し，$a \leq a$，

（ii）　$a \leq b,\ b \leq a \implies a = a$，

(iii) $a \leq b,\ b \leq c \implies a \leq c$.

特に，すべての $a, b \in A$ に対して，$a \leq b$ または $b \leq a$ であるとき，A は**全順序集合**（または線形順序集合）であるという．

半順序集合 A は次の条件をみたすとき，“帰納的に順序づけられている”という．

(I) A の部分集合 A_1 が全順序集合ならば，A_1 は上に有界である，すなわちある $a_0 \in A$ があって，$\forall a \in A_1$ に対し $a \leq a_0$.

次の補題は選択公理と同値である．（したがって，われわれはそれを公理として仮定する．）

ツォルンの補題．帰納的に順序づけられた（空でない）半順序集合 A は極大元をもつ．すなわち，ある $a_0 \in A$ があって，$a_0 \leq a$, $a \in A$ ならば，$a_0 = a$.

A 2.3. 第二の証明.

次のような組 (K, σ) を考える．

1) K は $F_1 \subset K \subset \overline{\boldsymbol{Q}}$ であるような体，

2) σ は K から $\overline{\boldsymbol{Q}}$ の中への（体の）同型写像で，$\sigma|F_1 = \sigma_0$ であるようなもの．

このような組 (K, σ) 全体の集合を $\mathcal{K}$ で表す．$(K, \sigma), (K', \sigma') \in \mathcal{K}$ に対し，

$$(K, \sigma) \leq (K', \sigma') \iff K \subset K',\ \sigma = \sigma'|K$$

によって $\leq$ を定義すれば，これは明らかに $\mathcal{K}$ の一つの半順序になる．

$\mathcal{K}$ は帰納的に順序づけられている．実際，$\mathcal{K}_1$ を $\mathcal{K}$ の部分集合で全順序集合になるものとすれば，次のようにその“上界”を構成することができる．まず

$$\widetilde{K} = \bigcup \{ K \mid (K, \sigma) \in \mathcal{K}_1 \}$$

とおけば，$\widetilde{K}$ は体になる．なぜならば，$\alpha, \beta \in \widetilde{K}$ とすれば，ある (K, σ), $(K', \sigma') \in \mathcal{K}_1$ があって，$\alpha \in K$, $\beta \in K'$. $\mathcal{K}_1$ は全順序集合であるから，

$$(K, \sigma) \leq (K', \sigma') \quad \text{または} \quad (K', \sigma') \leq (K, \sigma).$$

いま $(K, \sigma) \leq (K', \sigma')$ とすれば，$K \subset K'$ であるから，α, β はともに $\in K'$.

よって,

$$\alpha \pm \beta,\ \alpha\beta \in K' \subset \widetilde{K},$$

$$\alpha \neq 0 \text{ ならば, } \alpha^{-1} \in K' \subset \widetilde{K}.$$

$(K', \sigma') \leq (K, \sigma)$ のときも同様である. よって, $\widetilde{K}$ は体になる.

次に, $\alpha \in \widetilde{K}$ に対して, $\alpha \in K$ となるような $(K, \sigma) \in \mathscr{K}_1$ をとり

$$\widetilde{\sigma}(\alpha) = \sigma(\alpha)$$

とおく. これが well-defined であること, すなわち (K, σ) のとり方に関係しないこと, また $\widetilde{K}$ から $\overline{\boldsymbol{Q}}$ の中への同型になること, はただちにわかる. (考えてみて下さい.) このように定義された組 $(\widetilde{K}, \widetilde{\sigma})$ は確かに $\mathscr{K}$ に属する. すなわち, 上の条件 1), 2) をみたす. また定義から明らかに, すべての $(K, \sigma) \in \mathscr{K}_1$ に対し, $(K, \sigma) \leq (\widetilde{K}, \widetilde{\sigma})$ である. よって $(\widetilde{K}, \widetilde{\sigma})$ は $\mathscr{K}_1$ の上界になる.

したがってツォルンの補題により, $\mathscr{K}$ に極大元 (K_1, σ_1) が存在する. そこで $K_1 = K_1^{\sigma_1} = \overline{\boldsymbol{Q}}$ をいえば, $\sigma_1 \in G = \mathrm{Aut}(\overline{\boldsymbol{Q}})$ となって証明が終わる.

いま $K_1 \subsetneqq \overline{\boldsymbol{Q}}$ であったとし, $\alpha \in \overline{\boldsymbol{Q}}, \notin K_1$ をとる. α の K_1 における最小多項式を $f_0(x) \in K_1[x]$ とし, $f_0(x)$ の係数に σ_1 を施してえられる $K_1^{\sigma_1}$ の多項式を $f_0^{\sigma_1}(x)$, その一つの根を β とする. そのとき自然な同型

$$K_1(\alpha) \longrightarrow K_1[x]/(f_0(x)) \longrightarrow K_1^{\sigma_1}[x]/(f_0^{\sigma_1}(x)) \longrightarrow K_1^{\sigma_1}(\beta)$$

がえられる. これらの同型を合成してえられる同型を

$$\sigma_2 : K_1(\alpha) \longrightarrow K_1^{\sigma_1}(\beta)$$

とし, $K_2 = K_1(\alpha)$ とおけば, 明らかに

$$(K_2, \sigma_2) \in \mathscr{K}, \qquad (K_1, \sigma_1) \lneqq (K_2, \sigma_2)$$

となり, (K_1, σ_1) が極大元であることに矛盾する. よって $K_1 = \overline{\boldsymbol{Q}}$ である. そのとき, A2.1 におけると同じ論法により, $\sigma_1(K_1) = \overline{\boldsymbol{Q}}$ も成立する. (証終)

補遺3. p-進数体 $\boldsymbol{Q}_p$

A 3.1. 有理数の p-進附値. 有理数体 $\boldsymbol{Q}$ には，通常の絶対値の他に p-進附値というものが考えられる．これについてまず説明しよう．

素数 p を一つ固定する．$a \in \boldsymbol{Q}^\times$ を既約分数

$$a = \frac{b}{c}, \qquad b, c \in \boldsymbol{Z}, \quad (b, c) = 1$$

の形にかいたとき，b も c も p と互いに素ならば，a は“p と無縁である”ということにする．よく知られた素因数分解の一意性により，任意の $a \in \boldsymbol{Q}^\times$ は

(1) $$a = a'p^\nu, \qquad \nu \in \boldsymbol{Z}, \ \ a' \text{ は } p \text{ と無縁}$$

という形に一意的に表される．このとき，$\nu = \nu_p(a)$ とかく．また

(2) $$|a|_p = p^{-\nu_p(a)}$$

とおき，これを a の（正規化された）**p-進附値**という．特に $\nu_p(\pm 1) = 0$，$|\pm 1|_p = 1$．また

$$\nu_p(0) = \infty, \qquad |0|_p = 0$$

と定義する．

定義から明らかに，任意の $a, b \in \boldsymbol{Q}$ に対して

(3) $$|ab|_p = |a|_p |b|_p,$$

(4) $$|a+b|_p \leqq \mathrm{Max}\,(|a|_p, |b|_p)$$

が成立する．(4) は次のように証明される．$ab = 0$ のときは自明であるから，$a, b \neq 0$ とし，それらを (1) の形にかいて，$a = a'p^\nu$, $b = b'p^\mu$ とする．$\nu \leqq \mu$ ならば，

$$a+b = (a'+b'p^{\mu-\nu})p^{\nu}.$$

この括弧の中を c' とおけば，c' の分母は p を含まない．よって $\nu_p(a+b) \geqq \nu$, $|a+b|_p \leqq p^{-\nu} = |a|_p$ となる．（この場合，$\mathrm{Max}(|a|_p, |b|_p) = |a|_p$ である．）ここでもし $\nu<\mu$ ならば，c' は p と無縁になり，$\nu_p(a+b)=\nu$，したがって，(4) は等号で成立する．$\nu>\mu$ の場合にも同様に等号が成り立つ．

(4) からいわゆる三角不等式

$$|a+b|_p \leqq |a|_p + |b|_p$$

がでる．したがって，$\boldsymbol{Q}$ において2点 a, b の“距離”を $|a-b|_p$ と定義することにより，それは距離空間になる．したがって $\boldsymbol{Q}$ に新しい位相（p-進位相）が定義される．正数 ε を与えたとき，$a \in \boldsymbol{Q}$ の ε-近傍を

(5) $$U_{\varepsilon}(a) = \{x \in \boldsymbol{Q} \mid |x-a|_p < \varepsilon\}$$

によって定義するのである．(3), (4) からわかるように，$\boldsymbol{Q}$ における和や積はこの位相に関して連続である．

$\boldsymbol{Q}$ の p-進位相は通常の位相とは全然異なるものである．通常の位相に関して，$\boldsymbol{Z}$ は離散集合（各点が孤立点になる集合）であるが，p-進位相では

$$m = \lim_{\nu\to\infty}(m+p^{\nu})$$

であるから，各点が集積点になる．また，たとえば p-進位相では

$$(1-p)^{-1} = 1+p+p^2+\cdots$$

が成立するが，通常の位相（または q-進位相，$q \neq p$）では，この右辺はもちろん発散する．

A 3.2. 完備化. よく知られているように，実数体 $\boldsymbol{R}$ は有理数体 $\boldsymbol{Q}$ を通常の絶対値によって定義される距離に関して，完備化してえられる．これと全く同じことを上記の距離に関して行えば，p-進数体 $\boldsymbol{Q}_p$ がえられる．以下その要点を述べる．実数の場合と同様（むしろより簡単）であるから，順を追って証明していくことはそんなに難しくない．読者の演習問題としておこう．

1. $\boldsymbol{Q}$ の点列 $\{a_n\}$ に対し次の二つの条件は同値である．

1） $\forall \varepsilon > 0$ に対して，$\exists n_0 \in \boldsymbol{N}$ があって，

$$\forall n, m \geqq n_0 \implies |a_n - a_m|_p < \varepsilon.$$

2） $\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0.$

この条件が成立するとき，$\{a_n\}$ を**コーシー列**という．

2. $\boldsymbol{Q}$ のコーシー列全体の集合を R とかく．$\{a_n\}, \{b_n\} \in R$ に対して，

$$\{a_n\} + \{b_n\} = \{a_n + b_n\},$$

$$\{a_n\} \cdot \{b_n\} = \{a_n b_n\}$$

によって和と積を定義すれば，これらもまた R に属する．この演算に関して R は 1 をもつ可換環になる．

3. $\boldsymbol{Q}$ の点列 $\{a_n\}$ は 0 に収束する，すなわち $\lim_{n\to\infty} |a_n|_p = 0$ であるとき，“零列”であるという．零列はコーシー列であり，零列全体の集合 N は R のイデアルになる．

4. 商環 R/N は体になる．この体を **p-進数体** といい，$\boldsymbol{Q}_p$ で表す．

5. $a \in \boldsymbol{Q}$ に対し，$a_n = a$（$\forall n \in \boldsymbol{N}$）とおいてえられる点列はコーシー列になる．その $\bmod N$ の剰余類を $\iota(a)$ とかけば，写像 $\iota : \boldsymbol{Q} \to \boldsymbol{Q}_p$ は $\boldsymbol{Q}$ から $\boldsymbol{Q}_p$ の中への（体の）同型を与える．以後，この埋め込みにより $\boldsymbol{Q} \subset \boldsymbol{Q}_p$ と考えることにする．

6. コーシー列 $\{a_n\}$ に対し，$\lim_{n\to\infty} |a_n|_p$ が存在し，それは $\{a_n\}$ の $\bmod N$ の剰余類だけによって定まる．よって $\alpha = (\{a_n\} \bmod N)$ に対し

$$|\alpha|_p = \lim_{n\to\infty} |a_n|_p$$

と定義する．これを $\boldsymbol{Q}_p$ の（拡張された）“p-進附値”という．

7. $\boldsymbol{Q}_p$ の（拡張された）p-進附値に対しても (3), (4) が成立する．また，$a \in \boldsymbol{Q}$ に対してこの附値は本来の p-進附値 $|a|_p$ と一致する．

8. $\boldsymbol{Q}_p$ の p-進附値から定義される位相に関して，体の演算は連続である．（この意味で $\boldsymbol{Q}_p$ は“位相体”になる．）

9. $\alpha \in \boldsymbol{Q}_p$, $\alpha = (\{a_n\} \bmod N)$ とすれば，上の位相に関して，$\alpha = \lim_{n\to\infty} a_n$ である．したがって，$\boldsymbol{Q}$ は $\boldsymbol{Q}_p$ の中で稠密である．

10. $\boldsymbol{Q}_p$ は“完備”である．すなわち，$\boldsymbol{Q}_p$ において任意のコーシー列は収束する．（実際，$\boldsymbol{Q}_p$ におけるコーシー列 $\{\alpha_n\}$ が与えられたとき，9の稠密性により，$\forall n \in \boldsymbol{N}$ に対し，$|a_n - \alpha_n|_p < 2^{-n}$ となるような $a_n \in \boldsymbol{Q}$ をとることができる．そのとき，$\{a_n\}$ は $\boldsymbol{Q}$ におけるコーシー列になり，$\alpha = (\{a_n\} \bmod N)$ とおけば，$\lim_{n\to\infty} \alpha_n = \alpha$ である．）

以上により，$\boldsymbol{Q}_p$ を $\boldsymbol{Q}$ の“完備化”と考えることができる．しかも $\boldsymbol{Q}$ の p-進距離に関する完備化は（位相体の同型を除いて）一意的に定まることも証明される．

たとえば，$\boldsymbol{Q}_2$ において 17 は平方数で

$$\sqrt{17} = 1 + 2^3 + 2^5 + 2^6 + 2^7 + \cdots$$

（一般に，p 素数，$p \equiv \pm 1 \pmod 8$ ならば，$\boldsymbol{Q}_2$ の中に $\sqrt{\pm p}$ が存在する．工夫してみて下さい．）

A 3.3. p-進整数環 $\boldsymbol{Z}_p$.

p-進数体 $\boldsymbol{Q}_p$ において

(6) $$\boldsymbol{Z}_p = \{\alpha \in \boldsymbol{Q}_p \mid |\alpha|_p \leqq 1\}$$

をその“整数環”または“附値環”という．実際，(3), (4) からわかるように，これは $\boldsymbol{Q}_p$ の部分環になる．また $\boldsymbol{Z}_p$ のイデアルはすべて

(7) $$p^\nu \boldsymbol{Z}_p = \{\alpha \in \boldsymbol{Q}_p \mid |\alpha|_p \leqq p^{-\nu}\} \qquad (\nu \in \boldsymbol{Z},\ \nu \geqq 0)$$

で与えられることも容易に証明される．

$\boldsymbol{Q}_p$ における位相の定義から，$\{p^\nu \boldsymbol{Z}_p\ (\nu \in \boldsymbol{N})\}$ は $\boldsymbol{Q}_p$ における 0 の基本近傍系になっている．よって $\boldsymbol{Z}_p$ は開部分環で，したがって閉部分環でもある．（一般に位相群において，開部分群は同時に閉部分群でもある．）$p^\nu \boldsymbol{Z}_p$ も開かつ閉な部分環になる．したがって，4.9 におけると同様に $\boldsymbol{Q}_p$ は完全非連結な位相環である．

$0 < \varepsilon \leqq 1$ に対して $\nu \in \boldsymbol{Z}$ を，$p^{-\nu} \leqq \varepsilon < p^{-\nu+1}$ となるようにえらべば，$\nu \geqq 0$

で，(5) に定義した近傍は

$$U_\varepsilon(a) = a + p^\nu \boldsymbol{Z}_p$$

とかくことができる．

さて，任意の $\alpha \in \boldsymbol{Z}_p$ と $\nu \in \boldsymbol{N}$ を与えたとき，$\boldsymbol{Q}$ の稠密性によりある $a \in \boldsymbol{Z}_p \cap \boldsymbol{Q}$ があって，

$$\alpha \equiv a \pmod{p^\nu \boldsymbol{Z}_p}$$

となる．さらに，この a をそれと合同な $\boldsymbol{Z}$ の元でおきかえることができる．よって

(8) $$\boldsymbol{Z}_p = \boldsymbol{Z} + p^\nu \boldsymbol{Z}_p.$$

(この式から $\boldsymbol{Z}_p$ が $\boldsymbol{Z}$ の p-進位相に関する閉包であることがわかる．) 一方，明らかに

(9) $$\boldsymbol{Z} \cap p^\nu \boldsymbol{Z}_p = p^\nu \boldsymbol{Z}$$

であるから，環における "第2同型定理" により，同型

(10) $$\boldsymbol{Z}_p / p^\nu \boldsymbol{Z}_p \cong \boldsymbol{Z} / p^\nu \boldsymbol{Z}$$

がえられる．

さて，$\nu \leqq \mu$ のとき，自然な準同型

$$\tilde{\psi}_{\nu\mu} : \boldsymbol{Z}_p / p^\mu \boldsymbol{Z}_p \longrightarrow \boldsymbol{Z}_p / p^\nu \boldsymbol{Z}_p$$

が存在し，それは 5.1 で考えた自然な準同型

$$\psi_{\nu\mu} : \boldsymbol{Z} / p^\mu \boldsymbol{Z} \longrightarrow \boldsymbol{Z} / p^\nu \boldsymbol{Z}$$

と同型 (10) を通じて同じものになる．よって射影極限をとることにより，自然な（位相環の）同型

(11) $$\varprojlim_{\nu} \boldsymbol{Z}_p / p^\nu \boldsymbol{Z}_p \cong \varprojlim_{\nu} \boldsymbol{Z} / p^\nu \boldsymbol{Z}$$

がえられる．

さて任意の $\alpha \in \boldsymbol{Z}_p$ に対し，$\varprojlim_{\nu} \boldsymbol{Z}_p / p^\nu \boldsymbol{Z}_p$ の元

$$((\alpha \bmod p^\nu \boldsymbol{Z}_p))_{\nu \in \boldsymbol{N}}$$

を対応させることができる．この対応を (11) の同型と合成することにより，

自然な（連続）準同型

(12)
$$\varphi : \boldsymbol{Z}_p \longrightarrow \varprojlim_{\nu} \boldsymbol{Z}/p^\nu \boldsymbol{Z}$$

がえられる．$\bigcap_{\nu=1}^{\infty} p^\nu \boldsymbol{Z}_p = \{0\}$ であるから，φ は単射（一対一の写像）になる．一方，

$$a_\nu \in \boldsymbol{Z} \qquad (\nu \in \boldsymbol{N}),$$
$$((a_\nu \bmod p^\nu \boldsymbol{Z}))_{\nu \in N} \in \varprojlim_{\nu} \boldsymbol{Z}/p^\nu \boldsymbol{Z}$$

とすれば，$\nu \leqq \mu \Rightarrow a_\nu \equiv a_\mu \pmod{p^\nu}$ であるから，$\{a_\nu\}$ はコーシー列になり，$\alpha = (\{a_\nu\} \bmod N)$ とおけば，明らかに

$$\varphi(\alpha) = ((a_\nu \bmod p^\nu \boldsymbol{Z}))_{\nu \in N}$$

である．よって，φ は全射（上への写像）になる．$\boldsymbol{Z}_p$ の位相の定義からわかるように，φ は位相同型である．以上をまとめれば，

定理．(12) の準同型 φ は自然な（位相環の）同型を与える．

この定理から $\boldsymbol{Z}_p$ がコンパクトであることがわかる．したがって

$$\boldsymbol{Q}_p = \bigcup_{\nu=1}^{\infty} p^{-\nu} \boldsymbol{Z}_p$$

は局所コンパクトな位相体である．

(13)
$$\boldsymbol{Q}^{(p)} = \bigcup_{\nu=1}^{\infty} p^{-\nu} \boldsymbol{Z}$$

とおけば，これは分母が p のベキであるような有理数全体からなる部分環で，(10) から自然な（加群の）同型

(14)
$$\boldsymbol{Q}_p/\boldsymbol{Z}_p \cong \boldsymbol{Q}^{(p)}/\boldsymbol{Z}$$

がえられる．

さて，$\boldsymbol{Q}_p$ は局所コンパクトな位相加群として自己双対的である．実際，$\alpha, \xi \in \boldsymbol{Q}_p$ に対し，その内積を

(15)
$$\langle \alpha, \xi \rangle = \exp(2\pi i \cdot \psi(\alpha\xi \bmod \boldsymbol{Z}_p))$$

で定義すれば，写像

$$\alpha \longmapsto \chi_\alpha, \qquad \chi_\alpha(\xi) = \langle \alpha, \xi \rangle$$

により $\boldsymbol{Q}_p \cong \widehat{\boldsymbol{Q}}_p$ である．ここで ψ は（14）によって与えられる埋め込み

$$\psi : \boldsymbol{Q}_p/\boldsymbol{Z}_p \longrightarrow \boldsymbol{Q}^{(p)}/\boldsymbol{Z} \subset \boldsymbol{R}/\boldsymbol{Z}$$

を表す．

この自己双対性において，$\boldsymbol{Q}_p$ の（コンパクトな開）部分加群 $\boldsymbol{Z}_p$ の零化部分群は $\boldsymbol{Z}_p$ 自身になる．したがって，コンパクトな位相加群 $\boldsymbol{Z}_p$ の双対 $\widehat{\boldsymbol{Z}}_p$ は離散加群 $\boldsymbol{Q}_p/\boldsymbol{Z}_p$ であり，それは（(14) により）$\boldsymbol{Q}^{(p)}/\boldsymbol{Z}$ と同一視される．

補遺 4. 円分体のイデアル

A 4.1. 有限次代数体のイデアル. F を有限次代数体, $[F:\boldsymbol{Q}]=n$ とする. 6.2 の記号で, F の整数環を $\mathcal{O}_F=\mathcal{O}\cap F$ と表す. この節では $\mathcal{O}_F$ のイデアルに関する基本的なことを整理しておく.

定理 1.* $\mathcal{O}_F$ は $\boldsymbol{Z}$-加群として, n 個の元からなる底をもつ. すなわち, n 個の元 $\omega_1, \cdots, \omega_n \in \mathcal{O}_F$ があって, 任意の $\alpha \in \mathcal{O}_F$ は

$$\alpha = a_1\omega_1 + \cdots + a_n\omega_n, \qquad a_1, \cdots, a_n \in \boldsymbol{Z}$$

の形に一意的に表される. いいかえれば, 加群として $\mathcal{O}_F \cong \boldsymbol{Z}^n$ である.

証明は $\boldsymbol{Z}$-加群の理論から容易に導かれる. ([O], [T2] などを参照. $n=2$ の場合の例は 6.2, 定理 2.)

$\mathcal{O}_F$ のイデアルを $A, B, \cdots$ で表す. 特に $\alpha \in \mathcal{O}_F$ によって生成される単項イデアルを (α) で表す. いま, A を $\mathcal{O}_F$ の $\{0\}$ でないイデアル, $\alpha \in A, \alpha \neq 0$ とし, α の最小多項式を $f(x)=\sum a_i x^i$, $a_i \in \boldsymbol{Z}$ とすれば,

$$a_0 = -\sum_{i>0} a_i\alpha^i \in (\alpha) \subset A, \qquad a_0 \neq 0$$

であるから,

$$(a_0) \subset A \subset \mathcal{O}_F. \tag{1}$$

定理 1 により, $\mathcal{O}_F/(a_0) \cong (\boldsymbol{Z}/a_0\boldsymbol{Z})^n$ であるから

$$[\mathcal{O}_F : A] \leqq [\mathcal{O}_F : (a_0)] = |a_0|^n < \infty.$$

$[\mathcal{O}_F : A]=N(A)$ とおき, これをイデアル A の (絶対) **ノルム** という. 特に $N((a_0))=|a_0|^n$ である. $\mathcal{O}_F/A$ が有限(加)群であるから,

$$A \subset B \subset \mathcal{O}_F$$

となるようなイデアル B は有限個しかない．またそのようなイデアル B に対して，$N(B)$ は $N(A)$ の約数になる．任意の（$\{0\}$ でない）イデアル A に対しても n 個の元からなる底の存在が，定理1と（1）から証明される．

素イデアル，極大イデアルの概念は6.2に述べた．P が素イデアルであるとは，商環 $\mathcal{O}_F/P$ が零因子をもたないことであり，P が極大であるとは，$P \neq \mathcal{O}_F$ で，$\mathcal{O}_F/P$ が自明でないイデアルをもたないこと，すなわち体になることを意味する．したがって，一般に極大イデアルは素イデアルである．

$\mathcal{O}_F$ のイデアルに対してはこの逆もいえる．すなわち

定理2. $\mathcal{O}_F$ の（$\{0\}$, $\mathcal{O}_F$ と異なる）素イデアルは極大である．（以下，単に $\mathcal{O}_F$ の素イデアルというとき，$\{0\}$, $\mathcal{O}_F$ は除外することにする．）

（証明） P を素イデアルとし，$\xi \in \mathcal{O}_F$ に対し，その P を法とする剰余類を $[\xi] = \xi + P$ で表すことにする．$\alpha \in \mathcal{O}_F$ に対して写像

$$\psi_\alpha : [\xi] \longmapsto [\alpha][\xi] = [\alpha\xi]$$

は加群 $\mathcal{O}_F/P$ の自分自身への準同型である．$[\alpha] \neq 0$ とすれば，P が素であるから，ψ_α の核は $\{[0]\}$，すなわち ψ_α は一対一の対応になる．したがって，（$\mathcal{O}_F/P$ は有限加群であるから）ψ_α は上への写像にもなる．よってある $[\xi]$ に対して，$[\alpha][\xi] = [1]$，すなわち $[\alpha]$ は逆元をもつ．よって $\mathcal{O}_F/P$ は体になる．したがって P は極大である．（証終）

系. P, P' を素イデアル，$P \subset P'$ とすれば，$P = P'$．

定理3. A, B をイデアル，P を素イデアル，$AB \subset P$ とすれば，$A \subset P$ または $B \subset P$ である．

実際，$A \not\subset P$, $B \not\subset P$ とすれば，ある $\alpha \in A, \notin P$, $\beta \in B, \notin P$ が存在する．そのとき，$\alpha\beta \in AB \subset P$ となって P が素であることに反する．

定理4. 任意の（0でない）イデアル A に対して，いくつか（有限個）の素イデアル $P_1, P_2, \cdots, P_r$ があって，

(2)
$$P_1 P_2 \cdots P_r \subset A.$$

（証明） $N(A)$ に関する帰納法で証明する．A が素（または $= \mathcal{O}_F$）ならば

問題はない．A が素でなければ，ある $\beta, \gamma \in \mathcal{O}_F$ があって，$\beta, \gamma \notin A$，$\beta\gamma \in A$．そのとき

$$B = (\beta) + A, \qquad C = (\gamma) + A$$

とおけば，

$$B \supsetneqq A, \quad C \supsetneqq A, \qquad BC = (\beta\gamma) + (\beta)A + (\gamma)A + A^2 \subset A.$$

よって，$N(B), N(C) < N(A)$．帰納法の仮定により，素イデアル $P_1', \cdots, P_s'$；$P_1'', \cdots, P_t''$ があって

$$P_1' \cdots P_s' \subset B, \qquad P_1'' \cdots P_t'' \subset C$$

よって

$$P_1' \cdots P_s' P_1'' \cdots P_t'' \subset BC \subset A.$$

（証終）

系．A を $\{0\}$ でないイデアル，P を素イデアル，$A \subset P$ とすれば，あるイデアル A' があって

(3)　　$$PA' \subset A, \qquad A' \not\subset A.$$

実際，定理4において素イデアル $P_1, P_2, \cdots, P_r$ をその個数 r が最小になるようにとる．$A \subset P$ とすれば，定理3によりある i に対して，$P_i \subset P$，したがって $P_i = P$．簡単のため，$i = 1$ とする．そのとき $A' = P_2 \cdots P_r$ とおけば，(3) の条件が成り立つことは見やすい．

$\mathcal{O}_F$ の $\{0\}$ でないイデアル A に対して

(4)　　$$A^{-1} = \{\xi \in F \mid \xi A \subset \mathcal{O}_F\}$$

とおく．定義から明らかに A^{-1} は $\mathcal{O}_F$ を含む $\mathcal{O}_F$-加群である．また $\alpha \in A$，$\alpha \neq 0$ とすれば，$\alpha A^{-1} \subset \mathcal{O}_F$．

一般に，$B \subset F$ が次の二つの条件

(i)　B は $\{0\}$ でない $\mathcal{O}_F$-加群である；

(ii)　ある $\gamma \in F^{\times}$ があって，$\gamma B \subset \mathcal{O}_F$；

をみたすとき，B は $\mathcal{O}_F$ の**分数イデアル**であるという．上の A^{-1} は分数イデアルである．いままでの（$\{0\}$ でない）イデアルは，$\mathcal{O}_F$ に含まれる分数イデ

アルである(それを特に“整イデアル”ということもある). 分数イデアル B, C に対して, 整イデアルの場合と同様にして

$$B + C,\quad B \cap C,\quad BC$$

等が定義される. そしてこれらも分数イデアルになることが容易に証明される.

定理5. P を素イデアルとすれば,

$$P^{-1}P = \mathcal{O}_F \tag{5}$$

である.

(証明) 定義により $P^{-1}P$ は $\mathcal{O}_F$ の(整)イデアルで, $P \subset P^{-1}P$ である. P は極大であるから, $P^{-1}P = P$ または $P^{-1}P = \mathcal{O}_F$. よって, $P^{-1}P = P$ ではないことをいえばよい.

$P^{-1}P = P$ であったとする. P の一つの底を $\omega_1, \cdots, \omega_n$ とすれば, 任意の $\alpha \in P^{-1}$ に対して

$$\alpha\omega_j = \sum_{i=1}^{n} a_{ij}\omega_i, \qquad a_{ij} \in \mathbf{Z}$$

が成立する. よって, α は整行列 (a_{ij}) の特性多項式の根になる. したがって α の最小多項式も整係数になる(ガウスの補題*). よって $\alpha \in \mathcal{O}_F$. ゆえに $P^{-1} \subset \mathcal{O}_F$ である. 一方, $\beta \in P, \beta \neq 0$ とすれば, 定理4, 系により,

$$PB' \subset (\beta), \qquad B' \not\subset (\beta)$$

となるようなイデアル B' が存在する. $\gamma \in B', \notin (\beta)$ とすれば, $\gamma/\beta \notin \mathcal{O}_F$. しかし

$$\left(\frac{\gamma}{\beta}\right)P \subset \beta^{-1}PB' \subset \mathcal{O}_F$$

であるから, $\gamma/\beta \in P^{-1}$. よって $P^{-1} \not\subset \mathcal{O}_F$ となって上記と矛盾する. (証終)

系1. A を $\{0\}$ でないイデアル, P を素イデアル, $A \subset P$ とすれば, ある(整)イデアル A' があって

$$PA' = A, \qquad A' \supsetneq A. \tag{3'}$$

この第一の等式をみたすようなイデアル A' はただ一つ定まり，$A'=P^{-1}A$ で与えられる．

（証明）$A'=P^{-1}A$ とおけば，

$$PA' = PP^{-1}A = \mathcal{O}_F A = A.$$

逆に $PA'=A$ とすれば，

$$A' = \mathcal{O}_F A' = P^{-1}PA' = P^{-1}A$$

である．また

$$A' = P^{-1}A \subset P^{-1}P = \mathcal{O}_F.$$

$A' \supset A$ は明らかであるが，$A'=A$ とすれば，$P^{-1}A = A$ であるから，定理5の証明の中に述べたように $P^{-1} \subset \mathcal{O}_F$ となって矛盾である．　（証終）

系2. P を素イデアルとすれば，

$$\bigcap_{\nu=1}^{\infty} P^{\nu} = \{0\}. \tag{6}$$

（証明）$A=\bigcap_{\nu=1}^{\infty} P^{\nu}$ とおく．明らかに $PA=A$ が成立する．もし $A \neq \{0\}$ ならば，系1の記号で，$A'=P^{-1}A=A$ となって矛盾である．　（証終）

A 4.2. イデアル論の基本定理.

定理5が確立すれば，イデアル論の基本定理を証明することは容易である．

定理6 (Dedekind). $\mathcal{O}_F$ の $\{0\}$ でないイデアルは（$\{0\}$, $\mathcal{O}_F$ と異なる）素イデアルの積に分解される．このような分解は積の順序を除いて一意的である．

（証明）A を $\mathcal{O}_F$ の $\{0\}$ でないイデアルとする．まず，A の素イデアル分解の"存在"を $N(A)$ に関する帰納法で証明しよう．$A=\mathcal{O}_F$ のとき，A は0個の素イデアルの積であると考える．$A \neq \mathcal{O}_F$ のとき，A を含む（有限個の）イデアルのうち極大なものを一つとり，P_1 とする．P_1 は素イデアルである．$A_1=P_1^{-1}A$ とおけば，定理5, 系1により

$$P_1A_1 = A, \quad A \subsetneq A_1 \subset \mathcal{O}_F,$$

よって $N(A_1)<N(A)$ である．帰納法の仮定により素イデアル分解

$$A_1 = P_2\cdots P_r$$

が存在し，したがって

$$A = P_1A_1 = P_1P_2\cdots P_r.$$

次に，分解の“一意性”を（やはり $N(A)$ に関する帰納法によって）証明する．A の他の分解

$$A = P_1'P_2'\cdots P_{r'}'$$

があったとすれば，$A\subset P_1$ であるから，ある i があって，$P_1=P_i'$．簡単のため，$i=1$ とする．そのとき

$$P_2\cdots P_r = A_1 = P_1^{-1}A = P_2'\cdots P_{r'}'$$

であるから，帰納法の仮定により，$r=r'$ で，適当に番号をつけかえれば，

$$P_i = P_i' \qquad (2\leqq i\leqq r)$$

である． （証終）

定理 7． $\mathcal{O}_F$ の分数イデアル全体は積の演算に関して（可換）群になる．（この群を代数体 F の **イデアル群** という．）

（証明） 二つの分数イデアルの積がまた分数イデアルになることはすでに述べた．この積に関して結合の法則，交換の法則が成立することは明らかである．（実際，F の任意の部分加群の積に関してこれらの法則が成立する．） 任意の分数イデアル A に対して

$$A\mathcal{O}_F = A$$

が成立するから，$\mathcal{O}_F$ が単位元になる．$\beta\in F^{\times}$, $\beta A\subset\mathcal{O}_F$，その素イデアル分解を

$$\beta A = P_1\cdots P_r$$

とするとき，

$$A^* = \beta P_1^{-1}\cdots P_r^{-1}$$

とおけば，A^* は分数イデアルで（5）から容易にわかるように，

$$AA^* = \mathcal{O}_F$$

が成立する．よって，A^* が A の逆元になる．（実際，(4) の意味で $A^* = A^{-1}$ である.）　　（証終）

定理6, 7により $\mathcal{O}_F$ の任意の分数イデアル A は

(7)
$$A = P_1^{e_1}\cdots P_r^{e_r}, \quad e_i \in \boldsymbol{Z}, \neq 0$$
$$(P_1, \cdots, P_r \text{ は相異なる素イデアル})$$

の形に一意的に表されることが証明される．（すなわち，F のイデアル群は素イデアル全体によって生成される自由アーベル群になる.）（7）が成立するとき，任意の素イデアル P に対して

(8)
$$\nu_P(A) = \begin{cases} e_i & \exists i, P = P_i \text{ のとき} \\ 0 & \text{そうでないとき} \end{cases}$$

とおく．

定理8. $\mathcal{O}_F$ の二つの（$\{0\}$ でない）イデアル A, B に対して，次の三つの条件は同値である．

(i) $A \subset B$.

(ii) ∃整イデアル C があって，$A = BC$.

(iii) ∀素イデアル P に対して，$\nu_P(A) \geqq \nu_P(B)$.

（これらの条件が成立するとき，B は A の因子，または約数（約イデアル？）であるという.）

（証明）(i) ⇒ (ii)： $C = B^{-1}A$ とおけば，
$$C = B^{-1}A \subset B^{-1}B = \mathcal{O}_F, \qquad BC = BB^{-1}A = \mathcal{O}_F A = A.$$
(ii) ⇒ (i)： $A = BC$ とすれば，
$$A = BC \subset B\mathcal{O}_F = B.$$
(ii) ⇔ (iii) は基本定理から明白である．　　（証終）

系. B, C を $\{0\}$ でない（整）イデアルとすれば，その最大公約イデアル，最小公倍イデアルはそれぞれ $B+C$, $B\cap C$ で与えられる．

定理9. A, B, C を $\mathcal{O}_F$ の $\{0\}$ でない整イデアルとする．$A = BC$ ならば，

(9)
$$N(A) = N(B)N(C)$$

である.

（証明） $B=P$（素イデアル）のとき証明すれば十分である．そのとき，$A \subsetneq C$ であるから，ある $\gamma \in C$ があって，$\gamma \notin A$．$(\gamma)=CD$ とすれば，

$$D \subset \mathcal{O}_F, \qquad D \not\subset P$$

である．よって定理8系により

$$P+D=\mathcal{O}_F, \qquad P \cap D = DP$$

である．これらの等式に C を乗じて

$$A+(\gamma)=C, \qquad A \cap (\gamma) = (\gamma)P.$$

よって，環の第2同型定理により

$$C/A \cong (\gamma)/(\gamma)P.$$

明らかに加群の同型 $(\gamma)/(\gamma)P \cong \mathcal{O}_F/P$ が成立するから，

$$[C:A]=[\mathcal{O}_F:P]=N(P).$$

よって

$$N(A)=[\mathcal{O}_F:A]=[\mathcal{O}_F:C][C:A]=N(C)N(P).$$

（証終）

B, C が互いに素である（すなわち共通因子をもたない）ときには，

$$B+C=\mathcal{O}_F, \qquad B \cap C = BC$$

となるから，環の同型

(10) $$\mathcal{O}_F/B \times \mathcal{O}_F/C \cong \mathcal{O}_F/BC$$

が成り立つ（中国人の剰余定理）．この場合 (9) は (10) から明らかである．

問題1． 上の同型 (10) を証明せよ．

問題2． P を素イデアル，$\pi \in P, \pi \notin P^2$ とすれば，任意の $\nu \geqq 1$ に対して

(11) $$P^\nu = (\pi^\nu) + P^{\nu+1}$$

が成立する．この関係から

$$P^\nu/P^{\nu+1} \cong \mathcal{O}_F/P, \qquad N(P^\nu)=N(P)^\nu$$

を導け．

A 4.3. 円分体における素イデアル分解. この節では円分体 $F=\boldsymbol{Q}(\zeta_n)$ の整数環 $R=\mathcal{O}_F$ において，イデアル $(p)=pR$（p は素数）がどのように分解するかを調べる．$[F:\boldsymbol{Q}]=n_0$ とおく．（$n_0=\varphi(n)$ であることは以下の議論の副産物として示される．これは“円分多項式” $\Phi_n(x)\in\boldsymbol{Q}[x]$ (5.2,(28)) が既約であることを意味する.）

R における (p) の素イデアル分解を

(12)
$$(p)=P_1^{e_1}\cdots P_r^{e_r}$$

とする．両辺のノルムを比べれば，

$$N(pR)=p^{n_0}=N(P_1)^{e_1}\cdots N(P_r)^{e_r}.$$

よって $N(P_i)$ はいずれも p のベキになる．（これは $P_i\cap\boldsymbol{Z}=p\boldsymbol{Z}$，したがって $\boldsymbol{F}_p=\boldsymbol{Z}/p\boldsymbol{Z}\subset R/P_i$ となることからもわかる.） $N(P_i)=p^{f_i}$ とおけば，上式から

(13)
$$n_0=e_1f_1+\cdots+e_rf_r$$

という関係がえられる．

1）$(p,n)=1$ の場合. $G_n=\mathrm{Gal}(\boldsymbol{Q}(\zeta_n)/\boldsymbol{Q})$ とおく．$\sigma\in G_n$ は明らかに R を不変にする，すなわち $\sigma(R)=R$ である．分解 (12) の一つの素イデアル P_1 をとり

$$H_1=\{\sigma\in G_n\mid\sigma(P_1)=P_1\}$$

とおけば，H_1 は G_n の部分群である．（これを P_1 の“分解群”という.）$[G_n:H_1]=r_1$ とし，G_n の H_1 による (右) 傍系分解を

$$G_n=\bigcup_{i=1}^{r_1}\sigma_iH_1$$

とすれば，P_1 の共役のうち相異なるものは

$$\sigma_i(P_1)\qquad(1\leqq i\leqq r_1)$$

によって与えられる．これらの素イデアルはすべて (12) の分解の中に現れるから，$P_i=\sigma_i(P_1)$ $(1\leqq i\leqq r_1)$ としてよい．特に $r_1\leqq r$．また，

$$e_i = e_1, \quad f_i = f_1 \quad (1 \leqq i \leqq r_1)$$

である.

さて, R/P_1 は p^{f_1} 個の元からなる標数 p の体である. $\sigma \in H_1$ ならば, σ は R/P_1 の一つの自己同型を引き起こす. それを $\bar{\sigma}$ で表せば, 対応 $\sigma \mapsto \bar{\sigma}$ は準同型

(14) $$H_1 \longrightarrow \mathrm{Aut}(R/P_1)$$

を与える.

ここで (14) の準同型は一対一である. 実際, ある $\sigma \in H_1$ に対し, $\sigma \neq 1$, $\bar{\sigma} = 1$ であったとする. そのとき, $F = \boldsymbol{Q}(\zeta_n)$, $\zeta_n \in R^\times$ であることから,

$$\zeta_n^\sigma \neq \zeta_n, \quad \zeta_n^\sigma \equiv \zeta_n \pmod{P_1}$$

である. 5.2 の記号で $k = k(\sigma)$ $(\neq 1)$ とすれば,

$$\zeta_n^{k-1} \neq 1, \quad \zeta_n^{k-1} \equiv 1 \pmod{P_1}.$$

よって

$$n = \left.\frac{x^n - 1}{x - 1}\right|_{x=1} = \prod_{j=1}^{n-1} (\zeta_n^j - 1) \in P_1.$$

これは $P_1 \cap \boldsymbol{Z} = p\boldsymbol{Z}$, $(p, n) = 1$ に矛盾する.

(14) の準同型が一対一であるから,

$$|H_1| \leqq |\mathrm{Aut}(R/P_1)|$$

である. 有限体のガロア理論により, $\mathrm{Aut}(R/P_1)$ はフロベニウス同型 ($x \mapsto x^p$) によって生成される位数 f_1 の巡回群であることが知られている.* したがって $|H_1| \leqq f_1$. よって,

$$n_0 = |G_n| = [G_n : H_1] \cdot |H_1| \leqq r_1 f_1 = \sum_{i=1}^{r_1} f_i.$$

これと (13) とを比較して

(15) $$r_1 = r, \quad |H_1| = f_1, \quad e_i = 1 \quad (1 \leqq i \leqq r)$$

であることが結論される. 特に (14) の準同型は同型になる:

(14′) $$H_1 \cong \mathrm{Aut}(R/P_1).$$

(14′) によれば，ある $\sigma\in H_1$ に対して $\bar{\sigma}$ はフロベニウス同型になる．この σ に対して $k(\sigma)\equiv p\ (\mathrm{mod}\ n)$ であるから $\sigma=\sigma_p$ とかく．$(\boldsymbol{Z}/n\boldsymbol{Z})^\times$ は（いくつかの）$[p]=(p \bmod n\boldsymbol{Z})$，$(p,n)=1$ によって生成されるから，写像 $\sigma\mapsto k(\sigma)$ が定義する準同型

$$G_n \longrightarrow (\boldsymbol{Z}/n\boldsymbol{Z})^\times$$

は（上への）同型になる．よって，位数を比べて $n_0=\varphi(n)$．（したがって $\Phi_n(x)$ は既約である！）また f_1 は σ_p の位数，すなわち $[p]$ の位数と一致するから，

(16) $$p^{f_1}\equiv 1 \quad (\mathrm{mod}\ n)$$

となるような最小の自然数として特徴づけられる．

以上を要約すれば次の定理がえられる．

定理10． $(p,n)=1$ の場合，$\boldsymbol{Q}(\zeta_n)$ の整数環 R における (p) の素イデアル分解は

(17) $$(p)=P_1\cdots P_r,\qquad N(P_i)=p^{f_1},\qquad rf_1=\varphi(n)$$

の形になる．$P_i\ (1\leqq i\leqq r)$ は P_1 と共役なイデアルの全体である．また f_1 は (16) をみたす最小の自然数である．

2) $n=p^\nu$ の場合． この場合

(18) $$\Phi_n(x)=\frac{x^{p^\nu}-1}{x^{p^{\nu-1}}-1}=\prod_{k=0}^{p-1}x^{p^{\nu-1}k}$$

であるから，

(19) $$\Phi_n(1)=\prod_k{}^*(1-\zeta_n^k)=p,$$

ここで $\prod_k{}^*$ は $1\leqq k\leqq p^\nu$，$(k,p)=1$ にわたる積を表す．このような k に対して ζ_n^k はいずれも 1 の原始 p^ν 乗根であるから

$$\frac{1-\zeta_n^k}{1-\zeta_n}\in R^\times$$

である．よって，$1-\zeta_n$ が生成する R の単項イデアルを

(20) $$P_0 = (1-\zeta_n)$$

とおけば，

$$(p) = P_0^{e_0}, \qquad e_0 = \varphi(p^\nu)$$

である．この式の両辺のノルムを比較すれば

$$p^{e_0} = N(P_0)^{e_0}, \qquad \text{ゆえに} \qquad N(P_0) = p.$$

したがって P_0 は素イデアルである．以上により，

定理11． $n=p^\nu$ の場合，$\boldsymbol{Q}(\zeta_n)$ の整数環 R における (p) の素イデアル分解は

(21) $$(p) = P_0^{e_0}, \qquad e_0 = \varphi(p^\nu), \qquad N(P_0) = p$$

の形になる（すなわち (p) は R において“完全分岐”する）．P_0 は単項イデアル $(1-\zeta_n)$ である．

問題3． n が二つ以上の素数で割り切れるとき，$\Phi_n(1)=1$ であることを示せ．

3）一般の場合． $n=p^\nu n'$，$(p, n')=1$ とする．このとき，ある $u, v \in \boldsymbol{Z}$ があって

$$up^\nu + vn' = 1.$$

よって

$$\zeta_n = \zeta_{p^\nu}^v \zeta_{n'}^u.$$

したがって

$$\boldsymbol{Q}(\zeta_n) = \boldsymbol{Q}(\zeta_{p^\nu})\boldsymbol{Q}(\zeta_{n'})$$

である．

まず $\boldsymbol{Q}(\zeta_{p^\nu})$ の整数環における (p) の素イデアル分解を（21）とし，P_0 の $\boldsymbol{Q}(\zeta_n)$ の整数環 R への延長 P_0R の素イデアル分解を

$$P_0R = \prod_{i=1}^{r} P_i^{e_i'}, \qquad N(P_i) = p^{f_i}$$

とする．そのとき (p) の R における分解は

(22)
$$(p)=(P_0R)^{e_0}=\prod_{i=1}^{r}P_i^{e_0e_i'}$$

となる．

一方，$\boldsymbol{Q}(\zeta_{n'})$ の整数環 R' における (p) の素イデアル分解を

(17′)
$$(p)=\prod_{i=1}^{r'}P_i',\qquad N(P_i')=p^{f'},\qquad r'f'=\varphi(n')$$

とし，各 P_i' の R への延長を

$$P_i'R=\prod_{j=1}^{s_i}P_{ij}^{e_{ij}},\qquad N(P_{ij})=p^{f_{ij}}$$

とおけば，(p) の R における（もう一つの）素イデアル分解

(22′)
$$(p)=\prod_{i=1}^{r'}\prod_{j=1}^{s_i}P_{ij}^{e_{ij}}$$

がえられる．

容易にわかるように，

$$P_i'=P_{ij}\cap R',\qquad R'/P_i'\subset R/P_{ij}$$

であるから，P_{ij} はすべて相異なる素イデアルであり，$f'\leqq f_{ij}$ である．素イデアル分解の一意性により，(22), (22′) を比較して，$e_0\mid e_{ij}$．したがって，$e_{ij}=e_0e_{ij}'$ とおけば，

$$\sum_{i=1}^{r'}\sum_{j=1}^{s_i}e_{ij}'f_{ij}=\varphi(n').$$

しかし $r'f'=\varphi(n')$ であるから，

$$\forall i,\ \ s_i=1,\ \ e_{i1}'=1,\ \ f_{i1}=f'$$

でなければならない．したがって，また $r=r'$ で，適当に番号をつけかえれば

$$P_i=P_{i1},\qquad e_i'=1,\qquad f_i=f'\qquad(1\leqq i\leqq r)$$

となる．

以上をまとめて（f' を f とかき直して），

定理12. p を素数，$n=p^{\nu}n'$，$(p,n')=1$ とすれば，$\boldsymbol{Q}(\zeta_n)$ の整数環 R において，(p) の素イデアル分解は

$$(p)=\prod_{i=1}^{r}P_i^{e_0},\qquad N(P_i)=p^f, \tag{23}$$

$$e_0=\varphi(p^{\nu}),\qquad rf=\varphi(n')$$

の形になる．$P_1,\cdots,P_r$ は互いに共役な素イデアルである．$\boldsymbol{Q}(\zeta_{n'})$ の整数環を R'，$P_i\cap R'=P_i'$ とすれば，R' における (p) の素イデアル分解は

$$(p)=\prod_{i=1}^{r}P_i',\qquad N(P_i')=p^f \tag{17'}$$

で与えられ，$P_i'R=P_i^{e_0}$ である．

定理10, 12により，$\boldsymbol{Q}(\zeta_n)$ における (p) の分解法則は p の $\bmod n'$ の剰余類によって決定されることがわかる．

一般に定理12は次のような形に拡張される（ヒルベルトの理論*）．F を有限次代数体，F' をその有限次ガロア拡大，$[F':F]=n$ とする．P を $\mathcal{O}_F$ の素イデアルとすれば，P の $\mathcal{O}_{F'}$ への延長 $P\mathcal{O}_{F'}$ は次のように分解される．

$$P\mathcal{O}_{F'}=\prod_{i=1}^{r}P_i'^{e},\qquad N(P_i')=N(P)^f. \tag{24}$$

ここに r,e,f は正の整数で，$ref=n$．$P_1',\cdots,P_r'$ は互いに共役な（$\mathcal{O}_{F'}$ の）素イデアルで，$P_i'\cap\mathcal{O}_F=P$ である．

上と同様 P_1' の "分解群" を

$$H_1=\{\,\sigma\in\mathrm{Gal}(F'/F)\mid \sigma P_1'=P_1'\,\}$$

と定義し，(14) と同様な準同型

$$\varphi: H_1\longrightarrow \mathrm{Aut}(\mathcal{O}_{F'}/P_1')$$

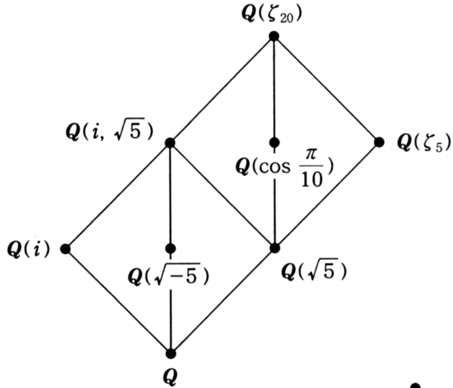
を考えれば，

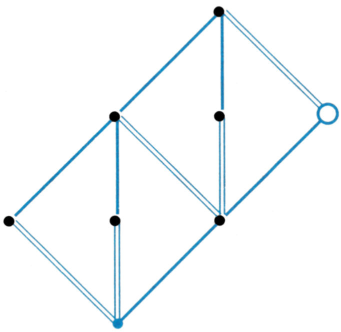
$$[\mathrm{Gal}(F'/F):H_1]=r,\qquad |H_1|=ef,$$

$$|\mathrm{Ker}\,\varphi|=e,\qquad |\mathrm{Im}\,\varphi|=f$$

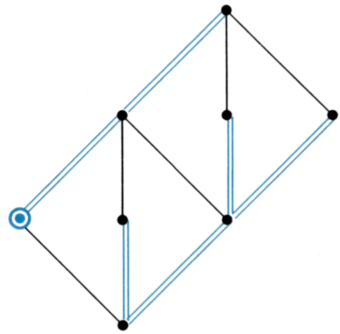
が成り立つ．$\mathrm{Ker}\,\varphi$ を P_1' の "惰性群" という．$\mathcal{O}_{F'}/P_1'$ は $\mathcal{O}_F/P$ の拡大体とみなされるが，それは f 次巡回拡大で，そのガロア群が $\mathrm{Im}\,\varphi$ と一致するのである．特に F'/F がアーベル拡大のときには，P_1' の分解群，惰性群は P だけによって定まるから，それらを P の分解群，惰性群ともいう．

$\boldsymbol{Q}(\zeta_{20})/\boldsymbol{Q}$ における素イデアルの変化図

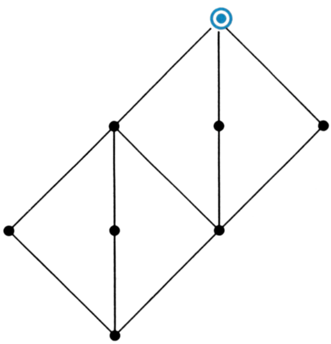




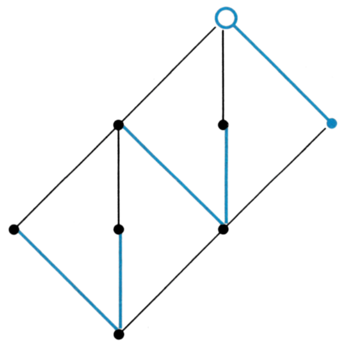
$p = 2$
$(2^4 \equiv 1 \quad (5))$



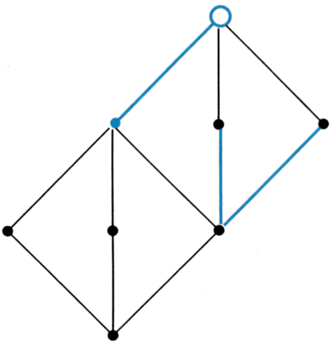
$p = 5$
$(5 \equiv 1 \quad (4))$



$p \equiv 1 \quad (20)$
$\left(\begin{array}{l} p \equiv 1 \quad (4) \\ p \equiv 1 \quad (5) \end{array}\right)$

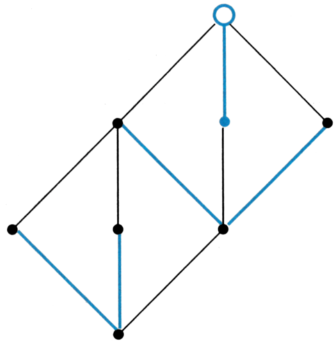


$p \equiv 11 \quad (20)$
$\left(\begin{array}{l} p^2 \equiv 1 \quad (4) \\ p \equiv 1 \quad (5) \end{array}\right)$



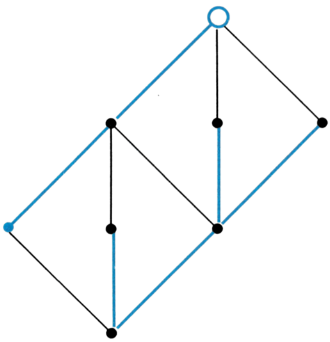
$p \equiv 9 \quad (20)$

$\begin{pmatrix} p \equiv 1 & (4) \\ p^2 \equiv 1 & (5) \end{pmatrix}$



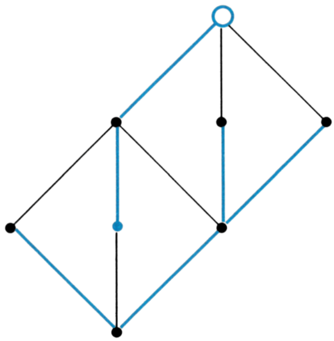
$p \equiv 19 \quad (20)$

$\begin{pmatrix} p^2 \equiv 1 & (4) \\ p^2 \equiv 1 & (5) \end{pmatrix}$



$p \equiv 13, 17 \quad (20)$

$\begin{pmatrix} p \equiv 1 & (4) \\ p^4 \equiv 1 & (5) \end{pmatrix}$



$p \equiv 3, 7 \quad (20)$

$\begin{pmatrix} p^2 \equiv 1 & (4) \\ p^4 \equiv 1 & (5) \end{pmatrix}$

$\boldsymbol{Q}(\zeta_{20})/\boldsymbol{Q}$ のガロア群は $(2, 2^2)$ 型のアーベル群である．$\boldsymbol{Q}$ の素数 p に対し，その $\boldsymbol{Q}(\zeta_{20})$ における素イデアル因子 $\widetilde{P}$ を一つ固定する．中間体 $\boldsymbol{Q} \subset F \subset F' \subset \boldsymbol{Q}(\zeta_{20})$, $[F' : F] = 2$ に対し，$\mathfrak{O}_F$ の素イデアル $P = \widetilde{P} \cap F$ の $\mathfrak{O}_{F'}$ における分解を考察する．このとき e, f, r のうちの一つが $=2$（他は $=1$）になるが，$e=2$ か $f=2$ か $r=2$ かに従って，F, F' を ═══，━━━，─── の線分で結ぶものとする．また，(p) の $\boldsymbol{Q}(\zeta_{20})/\boldsymbol{Q}$ における分解群，惰性群に対応する中間体（すなわち“分解体”，“惰性体”）を ●，○ で表すものとする．このような図式は $\widetilde{P}$ のとり方に無関係に（p だけで）定まる．この図からたとえば $\boldsymbol{Q}(\zeta_{20})$ に含まれる三つの 2 次体 $\boldsymbol{Q}(i)$, $\boldsymbol{Q}(\sqrt{-5})$, $\boldsymbol{Q}(\sqrt{5})$ における素数 p の分解の有様を読み取ることができる．

上に説明した円分体における分解法則は，通常，代数的整数論の教科書ではヒルベルトの理論，判別式の理論の応用として述べられている．しかし歴史的にいえば，順序は逆であって，これらの一般論は円分体の場合の事実を規範として構成されたものに違いない．ここではこの観点から，イデアル論の基本定理（と有限体に関する基本事項）だけから直接に円分体における分解法則を導いた．5.4で説明したように，これが類体論の原型なのであった．このように見るとき，円分体は代数的整数論の雄大な景観を見渡すために（アマチュアにも登ることのできる）絶好の展望台を提供しているということができよう．

後　書　き

参考文献.

[FMY]　藤崎源二郎・森田康夫・山本芳彦：数論への出発（入門｜現代の数学5），日本評論社，1980

[K]　河田敬義：19世紀の数学，整数論（数学の歴史Ⅶa），共立出版，1992

[M]　松坂和夫：代数系入門，岩波書店，1976

[N]　永尾　汎：代数学（新数学講座4），朝倉書店，1983

[O]　小野　孝：数論序説，裳華房，1987

[P]　L.S. ポントリャーギン（柴田泰光・杉浦光夫・宮崎功共訳）：連続群論，上，下，岩波書店，1957，1958

[Sc]　L. シュワルツ（吉田耕作・渡辺二郎訳）：物理数学の方法，岩波書店，1966

[Se]　J.-P. セール（彌永健一訳）：数論講義，岩波書店，1979

[T1]　高木貞治：初等整数論講義（第2版），共立出版，1983

[T2]　高木貞治：代数的整数論（第2版），岩波書店，1971

[T3]　高木貞治：近世数学史談（第3版），共立全書，1970；同，（解説：杉浦光夫），岩波文庫，1995

[V]　ファン・デル・ヴェルデン（銀林浩訳）：現代代数学Ⅰ，Ⅱ，Ⅲ，東京図書，1959－60

[W]　A. Weil：L'intégration dans les groupes topologiques et ses applications, Actualités Sci. Ind., Hermann, 1940

本文中に（証明なしに）引用した定理など（* をつけた所）について，より詳しく知りたいと思う読者のために，上の文献の該当する箇所を引用しておく．

1章 p.15：単因子 —— [M] pp.217－218；[N] p.126，定理30.8；[V] Ⅲ，p.148

2章 p.41：アーベル群の基本定理 —— [M] p.218，定理14, 15；[N] p.55，定理15.17；[P] 上，p.34，定理2；[V] Ⅲ，§109

3章 p.59：ガウスの和の符号 —— [O] §39；[T1] §60；[T2] p.274

pp.59－60：アーベル群の双対性 —— [N] §15.2；[P] 上，§40

pp.62−63： テータ関数，モジュラー形式 —— [Se] 第7章；[FMY] 第5章．(テータ関数は元来二つの複素変数の関数であるが，ここでは第2の変数を0としたもの，いわゆる Theta Nullwert を考える．)

4章 p.73： 代数学の基本定理 —— [M] p.322，§7；[N] p.163，定理37.11；[O] p.226，ノートB；[V] II，pp.293，298

p.77： 定理9 —— [M] p.240，§4；[N] p.140，問33.1，p.145，例題33.14
定理10 —— [M] p.266，§10；[N] p.158，定理36.13；[V] I，§40

5章 p.94： $\Phi_n(x)$ の既約性 —— [M] p.275，定理17；[N] p.167，定理39.4；[T1] §16；[V] II，pp.209−210

p.98： 類体論 —— [T2] 第11−16章；[T3] 付録1；[O] p.96

p.102： 正確には，(39′) の同型を φ，(36′) の極限としてえられる同型を φ' とするとき，$\varphi'(x)=\varphi(x)^{-1}$ という関係が成立する．

6章 p.104： 2次体の整数論 —— [FMY] 第3章；[O]；[T1] 第4−5章；[T2] p.249，付録(1)

p.106： $\mathcal{O}$ が環になること —— [V] III，pp.108−109；[O] p.35，定理1.22；[T2] p.7，定理1

p.107： イデアル論の基本定理 —— [O] §23；[T2] p.24，定理3，p.280，付録(3)；[V] III，§102．(本書補遺A4.1−4.2 の証明は大体において [V] に従った．)

pp.115−116： $\boldsymbol{Q}(\sqrt{5})$，$\boldsymbol{Q}(\sqrt{-3})$ の整数環が P.I.D. であること —— [M] p.144，問題3；[V] I，pp.77−78；[T1] p.303，例

p.116： Dirichlet の単数定理 —— [O] p.117，定理3.4；[T1] p.312，定理5.25；[T2] p.115，定理

p.117： 類数の有限性 —— [O] p.76，定理2.13；[T1] p.300，定理5.19；[T2] p.43，定理2

A4 p.138： $\mathcal{O}_F$ が底をもつこと —— [V] III，pp.112−114；[O] p.70，定理2.11；[T2] p.13，定理

p.141： ガウスの補題 —— [M] p.160，補題O；[N] p.105，補題26.9；[V] I，§23

p.147： 有限体のガロア理論 —— [M] p.271；[N] p.165，定理38.3；[O] §21

p.151： ヒルベルトの理論 —— [T2] §§8.2−8.4；[O] §27

なお，本書後半の主題であった代数的整数論（2次体，円分体，類体論）の成立の歴史については [K]，[FMY] を，さらにその黎明期（19世紀前半，ガウスの時代）については [T3] を読まれることをおすすめする．

索　引

あ　行

か　行

さ　行

著者紹介

佐武一郎（さたけ・いちろう）

1927年　山口県に生まれる
1950年　東京大学理学部数学科卒業
　　　　東京大学，シカゴ大学，カリフォルニア大学，東北大学などの教授を経て
現　在　中央大学理工学部教授
主　著　線型代数学（裳華房），Algebraic Structures of Symmetric Domains（岩波書店，Princeton Univ. Press），リー群の話（日本評論社）

代数学への誘い

1996年1月25日　第1版第1刷発行

定価はカバーに
表示しています

著　者　佐武一郎
発行者　西原昌幸
発行所　遊星社
〒164 東京都中野区中野3－50－1
電話（03）3381-5914　振替 00140-5-137657

発売元　星雲社
〒112 東京都文京区小石川5－19－25
電話（03）3947-1021　Fax（03）3947-1617

印刷・製本＝平河工業社　ISBN4-7952-6879-7